

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-242122

(P2003-242122A)

(43) 公開日 平成15年8月29日 (2003.8.29)

(51) Int.Cl.<sup>7</sup>

G 0 6 F 15/00

識別記号

3 3 0

3 1 0

F I

G 0 6 F 15/00

テームコード\* (参考)

3 3 0 C 5 B 0 8 5

3 1 0 D

審査請求 未請求 請求項の数16 O L (全 36 頁)

(21) 出願番号 特願2002-41080(P2002-41080)

(22) 出願日 平成14年2月19日 (2002.2.19)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 後藤 和裕

東京都品川区北品川6丁目7番35号 ソニ

一株式会社内

(72) 発明者 黒岩 達雄

東京都品川区北品川6丁目7番35号 ソニ

一株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

最終頁に続く

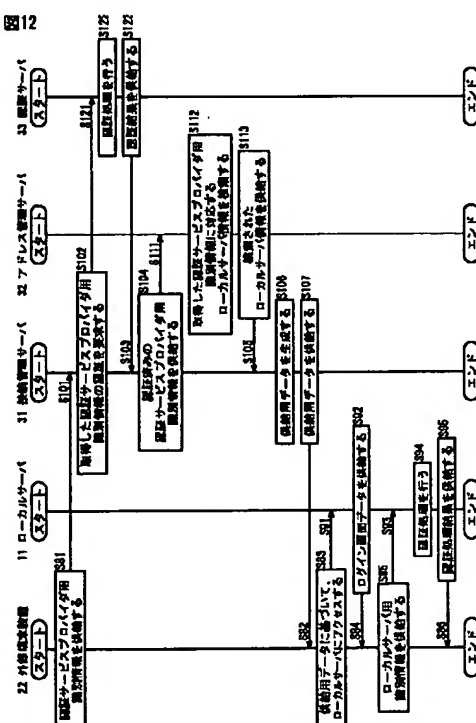
(54) 【発明の名称】 ネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラム

(57) 【要約】

【課題】 より安全に通信を行う。

【解決手段】 外部端末装置は、ステップS 8 1において、認証サービスプロバイダの接続管理サーバにアクセスし、認証サービスプロバイダ用識別情報を供給する。接続管理サーバは、認証サーバに認証処理を行わせ、取得した認証サービスプロバイダ用識別情報に対応するローカルサーバ情報をアドレス管理サーバより取得し、接続管理サーバは、ステップS 1 0 7において、取得したローカルサーバ情報に基づいて生成された、ローカルサーバのログイン画面のアドレス情報が含まれている供給用データを、外部端末装置に供給する。外部端末装置は、ステップS 8 3において、供給用データに基づいて、ローカルサーバにアクセスする。

図12



**【特許請求の範囲】**

**【請求項1】** ネットワークに接続され、他の情報処理装置と通信を行う第1の情報処理装置と、前記ネットワークに接続され、前記他の情報処理装置による、前記第1の情報処理装置への接続を管理する第2の情報処理装置とを備えるネットワークシステムであって、前記第1の情報処理装置は、前記他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、前記アドレス設定手段により設定された前記アドレスに関する情報を前記第2の情報処理装置に供給する第1の供給手段と、前記アドレスにアクセスした前記他の情報処理装置より供給される第1の識別情報の認証を行う第1の認証処理手段と、前記第1の認証処理手段による認証結果に基づいて、前記他の情報処理装置との接続を制御する接続制御手段とを備え、前記第2の情報処理装置は、前記第1の供給手段により供給された前記アドレスに関する情報を取得する第1の取得手段と、前記第1の取得手段により取得された前記アドレスに関する情報を記憶する記憶手段と、前記他の情報処理装置により供給される前記第1の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、前記接続要求受付手段により受け付けられた前記接続要求の要求元である前記他の情報処理装置より第2の識別情報を取得する第2の取得手段と、前記第2の取得手段により取得された前記第2の識別情報の認証を行う第2の認証処理手段と、前記第2の認証処理手段により前記第2の識別情報が認証された前記他の情報処理装置に、前記第2の識別情報に対応する、前記記憶手段により記憶されている前記アドレスに関する情報を供給する第2の供給手段とを備えることを特徴とするネットワークシステム。

**【請求項2】** ネットワークに接続され、第1の他の情報処理装置と通信を行う情報処理装置であって、前記第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、前記アドレス設定手段により設定された前記アドレスに関する情報を第2の他の情報処理装置に供給するアドレス情報供給手段と、前記アドレスにアクセスした前記第1の他の情報処理装置より供給される識別情報の認証を行う認証処理手段と、前記認証処理手段による認証結果に基づいて、前記第1の他の情報処理装置との接続を制御する接続制御手段とを備えることを特徴とする情報処理装置。

**【請求項3】** 前記アクセスを受け付けるアドレスは、前記情報処理装置に割り当てられたIPアドレスを含む基本アドレス、および、任意の文字列により構成される接続鍵を含み、前記アドレス設定手段は、前記基本アドレスを設定する基本アドレス設定手段と、前記接続鍵に関する設定を行う接続鍵設定手段とを備えることを特徴とする請求項2に記載の情報処理装置。

**【請求項4】** 前記接続鍵設定手段は、ユーザの指示に基づいて、前記ユーザにより入力された前記任意の文字

列を用いて前記接続鍵を設定することを特徴とする請求項3に記載の情報処理装置。

**【請求項5】** 前記接続鍵設定手段は、任意の文字列を生成する文字列生成手段を備え、前記ユーザの指示に基づいて、前記文字列生成手段により生成された前記文字列を用いて、前記ユーザが指示する時間毎に、前記接続鍵を更新し、前記アドレス設定手段は、前記接続鍵設定手段により更新された前記接続鍵を用いて、前記アドレスに関する情報を更新し、前記アドレス情報供給手段は、前記アドレス設定手段により更新された、前記アドレスに関する情報を前記第2の他の情報処理装置に供給することを特徴とする請求項3に記載の情報処理装置。

**【請求項6】** 前記第2の他の情報処理装置に供給される認証鍵を取得する認証鍵取得手段と、前記認証鍵取得手段により取得された前記認証鍵を記憶する認証鍵記憶手段と、前記第2の他の情報処理装置に接続する際に、前記記憶手段により記憶されている前記認証鍵を前記第2の他の情報処理装置に供給する認証鍵供給手段とをさらに備え、前記認証鍵供給手段は、前記認証鍵取得手段により予め取得され、前記記憶手段により記憶されている前記認証鍵を前記第2の他の情報処理装置に供給し、前記アドレス情報供給手段は、前記認証鍵供給手段により供給された前記認証鍵に基づいて接続された前記第2の他の情報処理装置に、前記アドレスに関する情報を供給することを特徴とする請求項2に記載の情報処理装置。

**【請求項7】** 接続を許可するユーザの識別情報を記憶する識別情報記憶手段をさらに備え、前記認証処理手段は、前記識別情報記憶手段により記憶されている前記識別情報を用いて、前記第1の他の情報処理装置より供給された前記識別情報の認証を行うことを特徴とする請求項2に記載の情報処理装置。

**【請求項8】** 前記アドレスに関する情報を含む接続情報を前記第1の他の情報処理装置に供給する接続情報供給手段をさらに備えることを特徴とする請求項2に記載の情報処理装置。

**【請求項9】** ネットワークに接続され、第1の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、前記第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第1の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする情報処理方法。

**【請求項10】** ネットワークに接続され、第1の他の

情報処理装置と通信を行う情報処理装置用のプログラムであって、前記第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第1の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項11】 ネットワークに接続され、第1の他の情報処理装置と通信を行う情報処理装置を制御するコンピュータが実行可能なプログラムであって、前記第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、前記アドレス設定ステップの処理により設定された前記アドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、前記アドレスにアクセスした前記第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、前記認証処理ステップの処理による認証結果に基づいて、前記第1の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とするプログラム。

【請求項12】 ネットワークに接続され、第1の他の情報処理装置による、第2の他の情報処理装置への接続を管理する情報処理装置であって、前記第2の他の情報処理装置より供給されたアドレスに関する情報を取得するアドレス情報取得手段と、前記アドレス情報取得手段により取得された前記アドレスに関する情報を記憶するアドレス情報記憶手段と、前記第1の他の情報処理装置により供給された前記第2の他の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、前記接続要求受け付け手段により受け付けられた前記接続要求の要求元である前記第1の他の情報処理装置から供給された識別情報を取得する識別情報取得手段と、前記識別情報取得手段により取得された前記識別情報の認証を行う識別情報認証処理手段と、前記識別情報認証処理手段により前記識別情報が認証された前記第1の他の情報処理装置に、前記識別情報に対応する、前記アドレス情報記憶手段により記憶されている前記アドレスに関する情報を供給するアドレス情報供給手段とを備えることを特徴とする情報処理装置。

【請求項13】 認証鍵を生成する認証鍵生成手段と、前記認証鍵生成手段により生成された前記認証鍵を、前記第2の他の情報処理装置に供給する認証鍵供給手段と、前記認証鍵生成手段により生成された前記認証鍵を、前記認証鍵供給手段により前記認証鍵を供給した前

記第2の他の情報処理装置に関する情報と関連付けて記憶する認証鍵記憶手段と、前記第2の他の情報処理装置より前記認証鍵を取得する認証鍵取得手段と、前記認証鍵記憶手段により記憶されている前記認証鍵を用いて、前記認証鍵取得手段により取得された前記認証鍵を認証する認証鍵認証手段と、前記認証鍵認証手段による認証結果に基づいて、前記第2の他の情報処理装置との接続を制御する接続制御手段とをさらに備え、前記アドレス情報取得手段は、前記接続制御手段による制御により接続された前記第2の他の情報処理装置から、前記アドレスに関する情報を取得することを特徴とする請求項12に記載の情報処理装置。

【請求項14】 ネットワークに接続され、第1の他の情報処理装置による、第2の他の情報処理装置への接続を管理する情報処理装置の情報処理方法であって、前記第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第1の他の情報処理装置により供給される前記第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第1の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする情報処理方法。

【請求項15】 ネットワークに接続され、第1の他の情報処理装置による、第2の他の情報処理装置への接続を管理する情報処理装置用のプログラムであって、前記第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第1の他の情報処理装置により供給される前記第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記

識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第1の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項16】 ネットワークに接続され、第1の他の情報処理装置による、第2の他の情報処理装置への接続を管理する情報処理装置を制御するコンピュータが実行可能なプログラムであって、前記第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、前記アドレス情報取得制御ステップの処理により取得が制御された前記アドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、前記第1の他の情報処理装置により供給される前記第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、前記接続要求受け付けステップの処理により受け付けられた前記接続要求の要求元である前記第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、前記識別情報取得制御ステップの処理により取得が制御された前記識別情報の認証を行う識別情報認証処理ステップと、前記識別情報認証処理ステップの処理により前記識別情報が認証された前記第1の他の情報処理装置への、前記識別情報に対応する、前記アドレス情報記憶制御ステップの処理により前記記憶部からの出力が制御されている前記アドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、ユーザ認証に用いられる識別情報を入力するための接続先アドレスを管理することによって、より安全に通信を行うことができるようにしたネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関する。

【0002】

【従来の技術】最近、インターネットの常時接続化やブロードバンド化とともに、家庭内等のローカルエリアにおいてもホームネットワークに代表されるLAN (Local Area Network) が普及してきている。ホームネットワークにおいては、通信機能を備えた家庭電化製品等が接続され、互いに情報を共有することができる。

【0003】通信機能を備えた家庭電化製品としては、例えば、パーソナルコンピュータの他に、ビデオテープ

レコーダ等の画像録画再生装置、テレビジョン受像機、オーディオ機器、照明機器、空調機器、またはゲーム機等、様々なものが存在する。これにより、ユーザは、例えば、パーソナルコンピュータでビデオの予約をしたり、照明の点灯および消灯を制御したりすることができる。

【0004】また、LANがインターネット等の外部のネットワークに接続されることで、LANに接続された機器同士で情報を共有するだけでなく、例えば、携帯電話機等からインターネットを介して、ホームネットワークに接続された家庭電化製品の動作を制御する等のように、外部の端末装置とも通信を行うことが可能になる。これによりユーザは、例えば、外出中であっても、携帯電話機を操作することで、自宅のパーソナルコンピュータが受信したメールを読んだり、テレビジョン放送の録画予約を行ったりすることができる。

【0005】このとき、ホームネットワークに接続された家庭電化製品には、例えば、IPv6(Internet Protocol version 6)を用いて、それぞれグローバルなIPアドレスを割り当てておく。携帯電話機は、外部のネットワークおよびホームネットワークを介して、それらのIPアドレスを用いて、各機器と通信を行うことができる。

【0006】しかしながら、この場合、家庭電化製品に割り当てられたIPアドレスが分かれば誰でも、外部のネットワークに接続された端末装置から、その家庭電化製品にアクセスすることができてしまう。

【0007】これに対して、サーバ等により、外部のネットワークからのアクセスに対してユーザ認証を行い、特定のユーザからのアクセスのみを許可する方法がある。この場合、そのサーバは、HTML (HyperText Markup Language) 等で記述されたWEBページを用いて、外部からアクセスしてきたユーザにID (Identification) やパスワード等の識別情報を入力させ、その識別情報を予め登録されているユーザ情報に基づいて認証することにより、ユーザ認証を行う。すなわち、ユーザは識別情報を入力するWEBページのURL (Uniform Resource Locator) にアクセスし、識別情報をサーバに供給する。

【0008】

【発明が解決しようとする課題】しかしながら、この場合、アクセス先のURLが固定されているため、セキュリティ上好ましくないという課題があった。例えば、許可されていない他のユーザでも、アクセス先のURLを知っていれば何度も識別情報の入力を試すことができるため、不正なログインを許可してしまう恐れがある。また、許可されていない他のユーザがアクセス可能な識別情報を入手した場合、その他のユーザは、サーバに登録されている情報を更新しない限り、容易に不正なログインを行うことができてしまう。

【0009】また、ユーザが複数のLANに対してアクセス可能な識別情報を有する等して、接続先が複数存在す

る場合、それらの接続先のURLや識別情報等を全て管理することが困難な場合があるという課題があった。例えば、複数の接続先が存在するユーザは、その接続先の数だけURLや識別情報を、記憶したりメモをとったりするなどして管理し、適切に使用しなければならないので、非常に煩雑な作業を要する場合がある。

【0010】本発明はこのような状況に鑑みてなされたものであり、より安全に通信を行うことができるようにするものである。

【0011】

【課題を解決するための手段】本発明のネットワークシステムは、ネットワークに接続され、他の情報処理装置と通信を行う第1の情報処理装置と、ネットワークに接続され、他の情報処理装置による、第1の情報処理装置への接続を管理する第2の情報処理装置とを備えるネットワークシステムであって、第1の情報処理装置は、他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、アドレス設定手段により設定されたアドレスに関する情報を第2の情報処理装置に供給する第1の供給手段と、アドレスにアクセスした他の情報処理装置より供給される第1の識別情報の認証を行う第1の認証処理手段と、第1の認証処理手段による認証結果に基づいて、他の情報処理装置との接続を制御する接続制御手段とを備え、第2の情報処理装置は、第1の供給手段により供給されたアドレスに関する情報を取得する第1の取得手段と、第1の取得手段により取得されたアドレスに関する情報を記憶する記憶手段と、他の情報処理装置により供給される第1の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、接続要求受付手段により受け付けられた接続要求の要求元である他の情報処理装置より第2の識別情報を取得する第2の取得手段と、第2の取得手段により取得された第2の識別情報の認証を行う第2の認証処理手段と、第2の認証処理手段により第2の識別情報が認証された他の情報処理装置に、第2の識別情報に対応する、記憶手段により記憶されているアドレスに関する情報を供給する第2の供給手段とを備えることを特徴とする。

【0012】本発明の第1の情報処理装置は、第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定手段と、アドレス設定手段により設定されたアドレスに関する情報を第2の他の情報処理装置に供給するアドレス情報供給手段と、アドレスにアクセスした第1の他の情報処理装置より供給される識別情報の認証を行う認証処理手段と、認証処理手段による認証結果に基づいて、第1の他の情報処理装置との接続を制御する接続制御手段とを備えることを特徴とする。

【0013】前記アクセスを受け付けるアドレスは、情報処理装置に割り当てられたIPアドレスを含む基本アドレス、および、任意の文字列により構成される接続鍵を含み、アドレス設定手段は、基本アドレスを設定する基

本アドレス設定手段と、接続鍵に関する設定を行う接続鍵設定手段とを備えるようにすることができる。

【0014】前記接続鍵設定手段は、ユーザの指示に基づいて、ユーザにより入力された任意の文字列を用いて接続鍵を設定するようにすることができる。

【0015】前記接続鍵設定手段は、任意の文字列を生成する文字列生成手段を備え、ユーザの指示に基づいて、文字列生成手段により生成された文字列を用いて、ユーザが指示する時間毎に、接続鍵を更新し、アドレス設定手段は、接続鍵設定手段により更新された接続鍵を用いて、アドレスに関する情報を更新し、アドレス情報供給手段は、アドレス設定手段により更新された、アドレスに関する情報を第2の他の情報処理装置に供給するようにすることができる。

【0016】前記第2の他の情報処理装置に供給される認証鍵を取得する認証鍵取得手段と、認証鍵取得手段により取得された認証鍵を記憶する認証鍵記憶手段と、第2の他の情報処理装置に接続する際に、記憶手段により記憶されている認証鍵を第2の他の情報処理装置に供給する認証鍵供給手段とをさらに備え、認証鍵供給手段は、認証鍵取得手段により予め取得され、記憶手段により記憶されている認証鍵を第2の他の情報処理装置に供給し、アドレス情報供給手段は、認証鍵供給手段により供給された認証鍵に基づいて接続された第2の他の情報処理装置に、アドレスに関する情報を供給するようにすることができる。

【0017】接続を許可するユーザの識別情報を記憶する識別情報記憶手段をさらに備え、認証処理手段は、識別情報記憶手段により記憶されている識別情報を用いて、第1の他の情報処理装置より供給された識別情報の認証を行うようにすることができる。

【0018】前記アドレスに関する情報を含む接続情報を第1の他の情報処理装置に供給する接続情報供給手段をさらに備えるようにすることができる。

【0019】本発明の第1の情報処理方法は、第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第1の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする。

【0020】本発明の第1の記録媒体のプログラムは、第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした



第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第1の他の情報処理装置との接続を制御する接続制御ステップとを含むことを特徴とする。

【0021】本発明の第1のプログラムは、第1の他の情報処理装置からのアクセスを受け付けるアドレスを設定するアドレス設定ステップと、アドレス設定ステップの処理により設定されたアドレスに関する情報の、第2の他の情報処理装置への供給を制御するアドレス情報供給制御ステップと、アドレスにアクセスした第1の他の情報処理装置より供給される識別情報の認証を行う認証処理ステップと、認証処理ステップの処理による認証結果に基づいて、第1の他の情報処理装置との接続を制御する接続制御ステップとをコンピュータに実行させる。

【0022】本発明の第2の情報処理装置は、第2の他の情報処理装置より供給されたアドレスに関する情報を取得するアドレス情報取得手段と、アドレス情報取得手段により取得されたアドレスに関する情報を記憶するアドレス情報記憶手段と、第1の他の情報処理装置より供給される第2の他の情報処理装置への接続要求を受け付ける接続要求受け付け手段と、接続要求受け付け手段により受け付けられた接続要求の要求元である第1の他の情報処理装置から供給された識別情報を取得する識別情報取得手段と、識別情報取得手段により取得された識別情報の認証を行う識別情報認証処理手段と、識別情報認証処理手段により識別情報が認証された第1の他の情報処理装置に、識別情報に対応する、アドレス情報記憶手段により記憶されているアドレスに関する情報を供給するアドレス情報供給手段とを備えることを特徴とする。

【0023】認証鍵を生成する認証鍵生成手段と、認証鍵生成手段により生成された認証鍵を、第2の他の情報処理装置に供給する認証鍵供給手段と、認証鍵生成手段により生成された認証鍵を、認証鍵供給手段により認証鍵を供給した第2の他の情報処理装置に関する情報と関連付けて記憶する認証鍵記憶手段と、第2の他の情報処理装置より認証鍵を取得する認証鍵取得手段と、認証鍵記憶手段により記憶されている認証鍵を用いて、認証鍵取得手段により取得された認証鍵を認証する認証鍵認証手段と、認証鍵認証手段による認証結果に基づいて、第2の他の情報処理装置との接続を制御する接続制御手段とをさらに備え、アドレス情報取得手段は、接続制御手段による制御により接続された第2の他の情報処理装置から、アドレスに関する情報を取得するようにすることができる。

【0024】本発明の第2の情報処理方法は、第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御され

たアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第1の他の情報処理装置により供給される第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第1の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする。

【0025】本発明の第2の記録媒体のプログラムは、第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御されたアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第1の他の情報処理装置より供給される第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第1の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとを含むことを特徴とする。

【0026】本発明の第2のプログラムは、第2の他の情報処理装置より供給されたアドレスに関する情報の取得を制御するアドレス情報取得制御ステップと、アドレス情報取得制御ステップの処理により取得が制御されたアドレスに関する情報の記憶部からの出力を制御するアドレス情報記憶制御ステップと、第1の他の情報処理装置より供給される第2の他の情報処理装置への接続要求を受け付ける接続要求受け付けステップと、接続要求受け付けステップの処理により受け付けられた接続要求の要求元である第1の他の情報処理装置から供給された識別情報の取得を制御する識別情報取得制御ステップと、識別情報取得制御ステップの処理により取得が制御された識別情報の認証を行う識別情報認証処理ステップと、識別情報認証処理ステップの処理により識別情報が認証された第1の他の情報処理装置への、識別情報に対応する、アドレス情報記憶制御ステップの処理により記

憶部からの出力が制御されているアドレスに関する情報の供給を制御するアドレス情報供給制御ステップとをコンピュータに実行させる。

【0027】本発明のネットワークシステムにおいては、ネットワークに接続され、他の情報処理装置と通信を行う第1の情報処理装置と、ネットワークに接続され、他の情報処理装置による、第1の情報処理装置への接続を管理する第2の情報処理装置とが備えられ、第1の情報処理装置においては、他の情報処理装置からのアクセスを受け付けるアドレスが設定され、設定されたアドレスに関する情報が第2の情報処理装置に供給され、アドレスにアクセスした他の情報処理装置より供給される第1の識別情報の認証が行われ、その認証結果に基づいて、他の情報処理装置との接続が制御され、第2の情報処理装置においては、取得されたアドレスに関する情報が記憶され、受け付けられた他の情報処理装置からの第1の情報処理装置への接続要求の要求元である他の情報処理装置より第2の識別情報が取得され、その第2の識別情報の認証が行われ、認証された他の情報処理装置に、第2の識別情報に対応するアドレスに関する情報が供給される。

【0028】本発明の第1の情報処理装置および方法、並びに第1のプログラムにおいては、第1の他の情報処理装置からのアクセスを受け付けるアドレスが設定され、設定されたアドレスに関する情報が第2の他の情報処理装置に供給され、アドレスにアクセスした第1の他の情報処理装置より供給される識別情報の認証が行われ、その認証結果に基づいて、第1の他の情報処理装置との接続が制御される。

【0029】本発明の第2の情報処理装置および方法、並びに第2のプログラムにおいては、取得された第2の他の情報処理装置より供給されたアドレスに関する情報が記憶され、第1の他の情報処理装置により供給された第2の他の情報処理装置への接続要求が受け付けられ、その接続要求の要求元である第1の他の情報処理装置から供給された識別情報が取得され、取得された識別情報の認証が行われ、識別情報が認証された第1の他の情報処理装置に、識別情報に対応するアドレスに関する情報が供給される。

【0030】

【発明の実施の形態】図1は本発明を適用したネットワークシステムの構成例を示す図である。

【0031】建物などに代表されるローカルエリア10に設置されたローカルサーバ11は、ホームネットワーク等に代表される、ローカルエリア10内のネットワークであるLAN12に接続されている。また、ローカルエリア10に設置された端末装置13もLAN12に接続されている。

【0032】LAN12は、図示せぬルータ等を介して、電話回線網やインターネット等に代表される、ローカル

エリア10の外部のネットワーク21に常時接続されている。

【0033】ローカルサーバ11は、LAN12を介して、例えば、端末装置13等、ローカルエリア10内に設置されているその他の機器の制御を行う。また、ローカルサーバ11は、ローカルエリア10の外部からのLAN12への接続を許可するユーザに関する情報を有しており、ネットワーク21から供給されたLAN12への接続要求を取得し、ユーザ認証を行う。

【0034】ネットワーク21には、パーソナルコンピュータ等の外部端末装置22が接続されており、外部端末装置22は、ネットワーク21を介してローカルサーバ11と通信を行い、ローカルサーバ11を制御したり、ローカルサーバ11を介して、LAN12に接続されている端末装置13を制御したりすることができる。

【0035】また、携帯電話機23は、ネットワーク21に接続された基地局24と無線通信を行うことにより、ネットワーク21と接続されており、この状態において、外部端末装置22と同様に、ネットワーク21を介してローカルサーバ11と通信を行い、ローカルサーバ11を制御したり、ローカルサーバ11を介して、LAN12に接続されている端末装置13を制御したりすることができる。

【0036】このとき、外部端末装置22や携帯電話機23は、ローカルサーバ11にアクセスするために、ネットワーク21を介して、認証サービスプロバイダ30に設置されている接続管理サーバ31と通信を行う。

【0037】認証サービスプロバイダ30は、ユーザ認証サービスを提供しており、ローカルエリア10の外部からローカルサーバ11へアクセスを行うユーザの認証処理を行う。

【0038】認証サービスプロバイダ30に設置されている接続管理サーバ31は、ネットワーク21に接続されており、ローカルエリア10の外部からのLAN12への接続要求を処理する。例えば、接続管理サーバ31は、外部端末装置22または携帯電話機23からのローカルサーバ11へのアクセスを管理する。

【0039】また、認証サービスプロバイダ30に設置されているアドレス管理サーバ32は、ネットワーク21を介してローカルサーバ11より供給されたローカルサーバ11に関する情報を管理する。また、アドレス管理サーバ32は、接続管理サーバ31にも接続されており、ローカルサーバ11に関する情報を接続管理サーバ31に供給することができる。

【0040】認証サービスプロバイダ30に設置されている認証サーバ33は、アドレス管理サーバ32に接続されており、認証サービスプロバイダ30へのアクセスに対してユーザ認証処理を行う。例えば、ローカルサーバ11がネットワーク21を介してアドレス管理サーバ32にアクセスした場合、認証サーバ33は、ローカル

サーバ11のユーザの認証処理を行う。また、例えば、外部端末装置22がネットワーク21を介して接続管理サーバ31にアクセスした場合、認証サーバ33は、アドレス管理サーバ32を介して接続管理サーバ31と通信を行い、外部端末装置22のユーザの認証処理を行う。

【0041】接続管理サーバ31、アドレス管理サーバ32、および認証サーバ33は、認証サービスプロバイダ30内において、互いに接続されているので、必要な情報を共有したり、処理を分散して実行させたりすることができる。

【0042】図2は、図1に示すローカルサーバ11の構成例を示すブロック図である。

【0043】図2において、CPU (Central Processing Unit) 51は、ROM (Read Only Memory) 52に記憶されているプログラム、または記憶部63からRAM (Random Access Memory) 53にロードされたプログラムに従って各種の処理を実行する。RAM 53にはまた、CPU 51が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU 51、ROM 52、およびRAM 53は、バス54を介して相互に接続されている。このバス54にはまた、入出力インタフェース60も接続されている。

【0044】入出力インタフェース60には、キーボード、マウスなどよりなる入力部61、CRT (Cathode Ray Tube)、LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどよりなる出力部62、ハードディスクなどにより構成される記憶部63、モデム、ターミナルアダプタ、またはLANアダプタなどにより構成される通信部64が接続されている。

【0045】記憶部63には、ユーザに関する情報等を含むデータや、各種の処理を実行するためのプログラム等が記憶されており、CPU 51に制御され、RAM 53にデータやプログラムを供給する。

【0046】通信部64は、LAN 12を介しての通信処理を行う。例えば、通信部64は、端末装置13とLAN 12を介して通信を行ったり、ローカルエリア10の外部の外部端末装置22とネットワーク21を介して通信を行ったりする。

【0047】入出力インタフェース60にはまた、必要に応じてドライブ70が接続され、磁気ディスク71、光ディスク72、光磁気ディスク73、或いは半導体メモリ74などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部63にインストールされる。

【0048】図3は、図1に示す外部端末装置22の構成例を示すブロック図である。

【0049】図3において、CPU 101は、ROM 102に記憶されているプログラム、または記憶部113からRAM 103にロードされたプログラムに従って各種の処理

を実行する。RAM 103にはまた、CPU 101が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU 101、ROM 102、およびRAM 103は、バス104を介して相互に接続されている。このバス104にはまた、入出力インタフェース110も接続されている。

【0050】入出力インタフェース110には、キーボード、マウスなどよりなる入力部111、ディスプレイやスピーカなどよりなる出力部112、ハードディスクなどにより構成される記憶部113、モデム、ターミナルアダプタなどにより構成される通信部114が接続されている。

【0051】記憶部113には、ローカルエリア10のローカルサーバ11にログインするのに必要なデータや、各種の処理を実行するためのプログラム等が記憶されており、CPU 111に制御され、RAM 113にデータやプログラムを供給する。

【0052】通信部114は、ネットワーク21を介しての通信処理を行う。例えば、通信部114は、ネットワーク21を介して、接続管理サーバ31やローカルサーバ11と通信を行う。

【0053】入出力インタフェース110にはまた、必要に応じてドライブ120が接続され、磁気ディスク121、光ディスク122、光磁気ディスク123、或いは半導体メモリ124などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部113にインストールされる。

【0054】図4は、図1に示す接続管理サーバ31の構成例を示すブロック図である。

【0055】図4において、CPU 151は、ROM 152に記憶されているプログラム、または記憶部163からRAM 153にロードされたプログラムに従って、ローカルエリア10の外部からのLAN 12への接続の管理に関する各種の処理を実行する。RAM 153にはまた、CPU 151が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU 151、ROM 152、およびRAM 153は、バス154を介して相互に接続されている。このバス154にはまた、入出力インタフェース160も接続されている。

【0056】入出力インタフェース160には、キーボード、マウスなどよりなる入力部161、ディスプレイやスピーカなどよりなる出力部162、ハードディスクなどにより構成される記憶部163、モデム、ターミナルアダプタなどにより構成される通信部164が接続されている。

【0057】記憶部163には、各種の処理を実行するためのプログラムやデータ等が記憶されており、CPU 151に制御され、RAM 153にデータやプログラムを供給する。

【0058】通信部154は、例えば、ネットワークを



介して外部端末装置22と通信処理を行う。また、通信部154は、アドレス管理サーバ32と接続されており、アドレス管理サーバ32と通信処理を行う。

【0059】入出力インタフェース160にはまた、必要に応じてドライブ170が接続され、磁気ディスク171、光ディスク172、光磁気ディスク173、或いは半導体メモリ174などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部163にインストールされる。

【0060】図5は、図1に示すアドレス管理サーバ32の構成例を示す図である。

【0061】図5において、CPU201は、ROM202に記憶されているプログラム、または記憶部213からRAM203にロードされたプログラムに従って、ローカルサーバ11のアドレス管理に関する各種の処理を実行する。RAM203にはまた、CPU201が各種の処理を実行する上で必要なデータなども適宜記憶される。CPU201、ROM202、およびRAM203は、バス204を介して相互に接続されている。このバス204にはまた、入出力インタフェース210も接続されている。

【0062】入出力インタフェース210には、キーボード、マウスなどよりなる入力部211、ディスプレイやスピーカなどよりなる出力部212、ハードディスクなどにより構成される記憶部213、モデム、ターミナルアダプタなどにより構成される通信部214が接続されている。

【0063】通信部214は、例えば、ネットワーク21を介して、ローカルサーバ11との通信処理を行う。また、通信部214は、接続管理サーバ31および認証サーバ33と接続されており、それらとの通信処理を行う。

【0064】入出力インタフェース210にはまた、必要に応じてドライブ220が接続され、磁気ディスク221、光ディスク222、光磁気ディスク223、或いは半導体メモリ224などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部213にインストールされる。

【0065】次に動作を説明する。図1に示すネットワークシステムにおいて、LAN12を管理するローカルサーバ11のユーザ（図示せず）は、認証サービスプロバイダ30の会員であり、認証サーバ33にユーザ情報が登録されているとする。なお、ユーザがローカルサーバ11購入時、またはセットアップ時に自動的に登録されるようにしてもよい。認証サーバ33に登録されているローカルサーバ11のユーザは、接続管理サーバ31およびアドレス管理サーバ32にログインするIDおよびパスワードからなる認証サービスプロバイダ用識別情報を有している。

【0066】以上のようにして、認証サービスプロバイダ30の会員であり、認証サービスプロバイダ用識別情

報を有するユーザによりローカルサーバ11が新たに設置されたり、または初期化されたりした場合、ローカルサーバ11は、ネットワーク21を介してアドレス管理サーバ32に、ローカルサーバ11に関する情報を供給し、ローカルサーバ11を登録させる。

【0067】図1に示すローカルサーバ11によるローカルサーバ情報登録処理を、図6のフローチャートを参照して説明する。

【0068】最初に、ステップS1において、ローカルサーバ11のCPU51は、初期化処理を行い、ローカルサーバ11に関する情報であるローカルサーバ情報を生成する。

【0069】ローカルサーバ情報には、機種情報、対応するユーザに関する情報、アドレス情報、およびアクセスに必要な接続キーに関する情報等を含んでいる。

【0070】機種情報は、ローカルサーバ11の機種名、製品番号、または性能に関する情報等を含み、ユーザに関する情報は、アドレス管理サーバ32に接続した際に使用された認証サービスプロバイダ用識別情報や、その識別情報に対応する、既に登録されているユーザに関する情報等を含み、アドレス情報は、ローカルサーバ11に割り当てられたアドレスまたは、ログイン画面の初期アドレス等の情報を含み、接続キーに関する情報は、接続キーおよびその設定に関する情報を含んでいる。

【0071】次に、CPU51は、通信部64を制御して、認証サービスプロバイダ用識別情報を用いて、アドレス管理サーバ32にアクセスする。そして、ステップS3において、アドレス管理サーバ32より認証処理結果に関する情報を取得し、認証されたか否かを判定する。認証されたと判定した場合、CPU51は、ステップS4に進む。

【0072】ステップS4において、CPU51は、ローカルサーバ情報をアドレス管理サーバ32に供給し、サーバ用キーを要求する。サーバ用キーは、アドレス管理サーバ32が生成し、ローカルサーバ11に供給するキーであり、ローカルサーバ11がアドレス管理サーバ32にログインする際に使用される。

【0073】後述するように、ローカルサーバ11は、アドレス管理サーバ32に定期的に接続する場合があり、その場合、ローカルサーバ11は、認証サービスプロバイダ用識別情報を定期的にネットワーク32に流してしまうことになり、セキュリティ上好ましくない。従って、ローカルサーバ11が認証サービスプロバイダ用識別情報を用いてログインするのは、最初の1回だけにするようにする。すなわち、以降、ローカルサーバ11がアドレス管理サーバ32に再接続する際は、サーバ用キーを使用する。

【0074】なお、サーバ用キーは認証サーバ33に登録されているユーザ情報と関連付けて生成され、登録さ

れているので、ローカルサーバ11が再び初期化されるまで有効である。

【0075】アドレス管理サーバ32にサーバ用キーを要求したCPU51は、ステップS5に進み、サーバ用キーを取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過したり、エラーメッセージを取得したりした場合、CPU51は、ローカルサーバ情報登録処理を終了する。

【0076】サーバ用キーを取得したと判定した場合、CPU51は、ステップS6に進み、取得したサーバ用キーを、例えば、記憶部63に保存し、ローカルサーバ情報登録処理を終了する。

【0077】また、ステップS3において、認証されていないと判定した場合、CPU51は、ローカルサーバ情報登録処理を終了する。

【0078】以上に説明したローカルサーバ11によるローカルサーバ情報登録処理に対応して、アドレス管理サーバ32は、ローカルサーバ情報登録処理を実行する。

【0079】図1に示すアドレス管理サーバ32によるローカルサーバ情報登録処理を、図7のフローチャートを参照して説明する。

【0080】最初に、ステップS21において、アドレス管理サーバ32のCPU201は、ローカルサーバ11より接続を要求されたか否かを判定し、要求されたと判定するまで待機する。

【0081】ローカルサーバ11が、図6のステップS2において、アドレス管理サーバ32にアクセスし、接続を要求したと判定した場合、CPU201は、ステップS22に進み、取得した認証サービスプロバイダ用識別情報に基づいて、認証処理を行う。CPU201は、通信部214を制御して、認証サーバ33に取得した認証サービスプロバイダ用識別情報を供給し、ユーザ認証処理を実行させ、処理結果を取得する。

【0082】そして、CPU201は、ステップS23において、ローカルサーバ11より取得した認証サービスプロバイダ用識別情報が認証されたか否かを判定する。認証されたと判定した場合、CPU201は、ステップS24に進み、ローカルサーバ11の接続要求を許可し、接続処理を行う。このとき、処理結果をローカルサーバ11に供給する。ローカルサーバ11のCPU51は、供給された処理結果に基づいて、ステップS3において、認証されたか否かを判定する。

【0083】そして、図7のステップS25において、CPU201は、接続されたローカルサーバ11より、ローカルサーバ情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過したり、回線が電氣的に切断されたり、エラーメッセージを取得したりした場合、CPU201は、ローカルサーバ情報登録処理を終了する。

【0084】図6のステップS4において、ローカルサーバ11により供給されたローカルサーバ情報を取得したと判定した場合、CPU201は、ステップS26に進み、サーバ用キーを生成し、取得したローカルサーバ情報に関連付けて記憶部213に登録する。

【0085】なお、サーバ用キーは、ローカルサーバ情報に関連付けて記憶されており、後述するように、サーバ用キーを用いたユーザ認証においては、サーバ用キーの認証とサーバ用キーを供給した装置の認証が行われる。従って、ローカルサーバ11に割り当てられたサーバ用キーをその他の装置から使用することはできない。

【0086】サーバ用キーを生成し、登録したCPU201は、ステップS27において、通信部214を制御して、生成したサーバ用キーをローカルサーバ11に供給し、ローカルサーバ情報登録処理を終了する。

【0087】また、ステップS23において、認証サーバ33が認証サービスプロバイダ用識別情報の認証に失敗したと判定した場合、CPU201は、ステップS28に進み、エラー処理を行い、ローカルサーバ情報登録処理を終了する。

【0088】以上のようにして、ローカルサーバ11が初期化されると、ローカルサーバ11に関する情報からなるローカルサーバ情報がアドレス管理サーバ32に供給され、登録される。

【0089】以上のように登録されたローカルサーバ情報に含まれる接続キーに関する情報等により、後述するように、ログイン画面のアドレスが設定される。接続キーに関する情報は、ローカルサーバ11において、ユーザにより入力される。

【0090】図8は、ローカルサーバ11における、ユーザが接続キーに関する設定を行う設定画面の様子の例を示す図である。

【0091】図8において、設定画面251は、ユーザが接続キーに関する設定を入力するための画面であり、CPU51等に制御され、出力部62のディスプレイ等に表示されるGUI (Graphical User Interface) である。ユーザは、この設定画面251に基づいて、入力部61のキーボードやマウス等を操作して、設定情報等を入力する。

【0092】設定画面251においては、各種のタブが用意されており、ユーザがマウスを操作し、タブを選択することにより、様々な設定が行えるようになっている。図8においては、接続キータブ252が選択されており、接続キーに関する設定を行うことができるようになっている。

【0093】設定画面251の中央部には、接続キー設定欄253が表示されており、ユーザが、接続キーを設定するか否か、接続キーを使用する場合、その内容を自動で変更するか否か等の設定を選択的に行うことができるようになっている。また、自動で変更する場合、その

時間間隔も設定できるようになっている。

【0094】また、接続キー設定欄の下側には、接続キー入力欄254が設けられており、接続キー設定欄253において、接続キーの自動変更が行われないように設定されている場合、ユーザは、接続キー入力欄254に好みの接続キーを入力することができる。図8において、接続キー入力欄254には、文字列「04C3DAFA07234e3c94ECAC7800681515」が入力されている。

【0095】図9は、ローカルサーバ11における、ユーザが接続キーに関する設定を行う設定画面の様子の他の例を示す図である。

【0096】図9において、ユーザは、設定画面251の状態タブ261が選択されており、接続キーに関するサービスの制御を行えるようになっている。

【0097】設定画面251の状態タブ261の下には、接続キーに関するサービスの制御を行う、サービス制御設定欄262が設けられている。ユーザは、入力部61を操作して、サービスを開始したり、停止したり、再起動したりすることができる。

【0098】サービス制御設定欄262の下側には、ログイン画面のアドレス情報を表示するログイン画面URL表示欄263が設けられている。ログイン画面のURLは、基本のURLに接続キーを付加した構成となっている。すなわち、図9の場合、ログイン画面のURLは、基本のURL「http://00.11.222.3/aaa/bbb/cc?」に接続キー「04C3DAFA07234e3c94ECAC7800681515」を付加された構成となっており、「http://00.11.222.3/aaa/bbb/cc?LoginKey=04C3DAFA07234e3c94ECAC7800681515」と表示されている。なお、図9の場合、ログイン画面URL表示欄263には、通常のURLとSSL（Secure Socket Layer）対応のURLが表示されている。

【0099】SSLはインターネット等のネットワークで情報を暗号化して送受信するプロトコルであり、現在広く使われているWWW（World Wide Web）やFTP（File Transfer Protocol）などのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信するためのプロトコルである。SSLは公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことを目的としている。国際標準化機構により制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針に基づき、コンピュータの持つべき通信機能を階層構造に分割したモデルであるOSI（Open Systems Interconnection）参照モデルではトランスポート層（第4層）にあたり、HTTP（HyperText Transfer Protocol）やFTPなどの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

【0100】以上のように、ログイン画面のURLを構成することにより、例えば、接続キーを定期的に自動変更

するように設定しておくことで、ログイン画面のURLは定期的に変更されるので、第3者がIDやパスワードを入力しても、認証サービスプロバイダ用識別情報を取得していないとログイン画面を開くことができないため、不正なアクセスを抑制することができる。

【0101】ローカルサーバ11のユーザは、入力部61のキーボードやマウス等を操作して、出力部62のディスプレイ等に表示されている設定画面251に備えられているタブの中から、図8に示すように、接続キータブ252を選択し、接続キー設定欄253において、接続キーを使用するか否か、使用する場合は、接続キーを自動で変更するか否か、自動で変更する場合は、その変更を行う時間間隔を設定する。また、自動で変更しないと設定した場合、ユーザは、接続キー入力欄254に接続キーを入力する。なお、接続キーは、その文字数が制限されていてもよく、例えば128bitの32文字までの文字列または数字列などにより構成されるようにしてもよい。

【0102】図8に示す設定画面251の入力が完了したユーザは、次に、入力部61のキーボードやマウス等を操作して、状態タブ261を選択し、サービス制御設定欄262において、設定した接続キーのサービスを開始させる。なお、設定された接続キーおよびログイン画面のアドレス情報は、ログイン画面URL表示欄に表示される。

【0103】以上のように、ローカルサーバ11において、接続キーはユーザにより設定され、有効化される。有効化された接続キーは、ローカルサーバ情報に含められ、アドレス管理サーバ32に供給される。

【0104】以上のような接続キーに関する設定は、同様の操作を行うことで、いつでも更新することができる。そして、接続キーに関する設定が更新された場合、アドレス管理サーバ32に登録されているローカルサーバ情報も更新される。この更新処理は、ユーザの指示により、または、自動で定期的に行われる。

【0105】図1に示すローカルサーバ11によるローカルサーバ情報更新処理を、図10のフローチャートを参照して説明する。

【0106】最初に、ステップS41において、ローカルサーバ11のCPU51は、更新された接続キーをアドレス情報に付加し、記憶部63に記憶されているローカルサーバ情報を更新する。

【0107】そして、ステップS42において、CPU51は、更新したローカルサーバ情報に記憶部63に記憶しているサーバ用キーを付加し、通信部64を制御して、ネットワーク21を介してアドレス管理サーバ32に供給する。ローカルサーバ情報を供給したCPU51は、ステップS43に進み、アドレス管理サーバ32より、処理結果情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過した

場合、CPU 51は、ローカルサーバ情報更新処理を終了する。

【0108】処理結果情報を取得したと判定した場合、CPU 51は、ステップS 44に進み、取得した処理結果情報に基づいて、処理結果を出力部62のディスプレイ等に表示し、ローカルサーバ情報更新処理を終了する。

【0109】以上に説明したローカルサーバ11によるローカルサーバ情報更新処理に対応して、アドレス管理サーバ32もローカルサーバ情報更新処理を実行する。

【0110】図1に示すアドレス管理サーバ32によるローカルサーバ情報更新処理を、図11のフローチャートを参照して説明する。

【0111】アドレス管理サーバ32のCPU 201は、ステップS 61において、ローカルサーバ11が図10のステップS 42において供給したローカルサーバ情報およびサーバ用キーを、ネットワーク21を介して取得したか否かを判定し、取得したと判定するまで待機する。

【0112】ローカルサーバ11よりローカルサーバ情報およびサーバ用キーを取得したと判定した場合、CPU 201は、ステップS 62に進み、新たに取得したサーバ用キーを記憶部213に登録済みのサーバ用キーと比較し、認証処理を行う。なお、このとき、サーバ用キーの認証だけでなく、例えば、ローカルサーバ情報の内容からユーザ認証やローカルサーバ11の認証などを行うようにしてもよい。このように、複数の認証を行うことで、セキュリティをさらに向上させることができる。

【0113】認証処理が終了したCPU 201は、ステップS 63において、ユーザが認証されたか否かを判定する。そして、認証されたと判定した場合、CPU 201は、ステップS 64において、取得したアドレス情報に基づいて、記憶部213に登録されているローカルサーバ情報を更新する。

【0114】そして、ステップS 65において、CPU 201は、処理結果情報を作成し、ネットワーク21を介して、ローカルサーバ11に供給し、ローカルサーバ情報更新処理を終了する。

【0115】また、ステップS 63において、認証に失敗し、認証されていないと判定した場合、CPU 201は、ステップS 65に進み、処理結果情報を生成し、ローカルサーバ11に供給し、ローカルサーバ情報更新処理を終了する。

【0116】以上のようにして、ローカルサーバ情報更新処理が行われるので、接続キーを自動的に変更するように設定した場合においても、認証サービスプロバイダ用識別情報をネットワーク21に定期的に流出することを防止することができる。

【0117】次に、以上のように設定された接続キーを用いて、ローカルエリア10の外部よりネットワーク21を介してローカルサーバ11に接続する方法について

説明する。

【0118】外部端末装置22からネットワーク21を介してローカルサーバ11にログインする場合について、図12のタイミングチャートを参照して説明する。また、必要に応じて、図13乃至図16を参照して説明する。なお、外部端末装置22のユーザは、ローカルサーバ11に登録されており、IDおよびパスワード等からなる識別情報を有している。

【0119】最初に、外部端末装置22のCPU 101は、ステップS 81において、通信部114を制御して、ネットワーク21を介して認証サービスプロバイダ30の接続管理サーバ31にアクセスし、認証サービスプロバイダ用識別情報を供給する。

【0120】図13は、外部端末装置22が接続管理サーバ31にアクセスした際に、出力部112のディスプレイに表示されたWEBブラウザのログイン画面の例を示す図である。

【0121】図13において、ログイン画面281には、IDを入力するID入力欄282、パスワードを入力するパスワード入力欄283、ユーザが、入力部111のマウス等で操作することによりログインを指示するログインボタン284が表示されている。

【0122】ユーザが接続管理サーバ31の所定のアドレスにアクセスすると、接続管理サーバ31は、ネットワーク21を介して、図13に示すようなGUI情報を外部端末装置22に供給する。外部端末装置22は、そのGUI情報を取得すると、ディスプレイに表示されているWEBブラウザに図13に示すようなログイン画面281を表示させる。

【0123】外部端末装置22のユーザは、ID入力欄282およびパスワード入力欄283に、認証サービスプロバイダ用識別情報に含まれるIDおよびパスワードをそれぞれ入力し、マウス等でログインボタンを操作する。外部端末装置22のCPU 101は、ユーザによりログインボタン284が操作されると、入力されたIDおよびパスワードを、ネットワーク21を介して、接続管理サーバ31に供給する。

【0124】接続管理サーバ31のCPU 151は、ステップS 101において、供給された認証サービスプロバイダ用識別情報を取得する。そして、ステップS 102において、CPU 151は、認証サーバ33に、取得した認証サービスプロバイダ用識別情報を供給し、その認証を要求する。

【0125】図示せぬ認証サーバ33のCPUは、ステップS 121において、供給された認証サービスプロバイダ用識別情報を取得すると、ステップS 122において、その識別情報に対して認証処理を行う。そして、認証サーバ33のCPUは、ステップS 123において、その認証結果を接続管理サーバ31に供給する。

【0126】接続管理サーバ31のCPU 151は、ステ

ップS103において、通信部164を制御し、認証サーバ33より供給された認証結果を取得し、認証されたと判定すると、ステップS104において、認証済みの認証サービスプロバイダ用識別情報を、アドレス管理サーバ32に供給する。

【0127】ステップS111において、アドレス管理サーバ32のCPU201は、通信部214を制御して、供給された認証済み認証サービスプロバイダ用識別情報を取得すると、ステップS112において、記憶部213に登録されている、取得した認証サービスプロバイダ用識別情報に対応するローカルサーバ情報を検索する。

【0128】そして、CPU201は、ステップS113において、通信部214を制御して、検索されたローカルサーバ情報を、接続管理サーバ31に供給する。接続管理サーバ31のCPU151は、ステップS105において、通信部164を制御して、供給されたローカルサーバ情報を取得する。

【0129】ローカルサーバ情報を取得した接続管理サーバ31のCPU151は、ステップS106において、取得したローカルサーバ情報に基づいて、外部端末装置22に供給するための供給用データを生成する。供給用データには、外部端末装置22が供給した認証サービスプロバイダ用識別情報に対応するローカルサーバ11のログイン画面のアドレス情報が含まれている。このとき、識別情報に対応するログイン画面のアドレス情報が複数存在する場合、供給用データには、複数のアドレス情報が含まれる。

【0130】供給用データを生成した接続管理サーバ31のCPU151は、ステップS107において、通信部164を制御し、ネットワーク21を介して外部端末装置22に供給用データを供給する。

【0131】外部端末装置22のCPU101は、ステップS82において、通信部114を制御して、供給用データを取得すると、供給用データに基づいて、図14に示すような、接続先であるローカルサーバの一覧を、出力部112のディスプレイに表示されるWEBブラウザに表示させる。

【0132】図14は、WEBブラウザに表示されたローカルサーバ一覧画面の例を示す図である。

【0133】図14において、ローカルサーバ一覧画面291の中央には、外部端末装置22のユーザに対応してアドレス管理サーバ32に登録されているローカルサーバであるパーソナルコンピュータ（以下、PCと称する）の一覧を表示するローカルサーバ一覧表示欄292が設けられている。外部端末装置22のユーザが表示されているPCの中から目的のPCを選択し、マウス等でローカルサーバ一覧表示欄292内に表示されているアクセスボタン293を操作すると、CPU101は、通信部114を制御して、指示されたPCにアクセスする。

【0134】また、ローカルサーバ一覧画面291のロ

ーカルサーバ一覧表示欄292の右上に設けられた更新ボタン294を、ユーザがマウス等で操作すると、CPU101は、ローカルサーバ一覧表示欄292に表示されている情報を更新し、最新のPCの一覧情報を表示する。

【0135】さらにローカルサーバ一覧表示欄292の下側には、詳細情報表示ボタン295が設けられており、ユーザがマウス等でこの詳細情報表示ボタン295を操作すると、例えば、ローカルサーバ一覧表示欄292に表示されているPCのアドレス情報や機種情報等の詳細情報が表示される。また、ローカルサーバ一覧表示欄292に表示されているPCの登録を解除することもできる。ユーザが表示されたGUIに基づいてPCの登録を解除すると、ローカルサーバ一覧画面291のローカルサーバ一覧表示欄292からそのPCが削除される。

【0136】また、ローカルサーバ一覧画面291の右上部には、SSL解除ボタン296とログアウトボタン297が設けられている。

【0137】外部端末装置22は、通常、ローカルサーバ11にSSLを用いて情報を暗号化して接続を行う。ユーザがマウス等によりSSL解除ボタン296を操作すると、外部端末装置22は、SSLによる暗号化を行わずにローカルサーバ11と通信を行うことができる。これにより、SSLを用いた暗号化による負荷をかけずに通信を行うことができるので、例えば、外部端末装置22の処理能力が高くない場合であっても、ローカルサーバ11と通信を行うことができる。

【0138】また、ユーザがマウス等によりログアウトボタン297を操作すると、外部端末装置22は、接続されている接続管理サーバ31からログアウトし、ローカルサーバ11への接続処理を中断する。

【0139】図12に戻り、外部端末装置22のユーザが、以上のようなローカルサーバ一覧画面291より接続するPCを選択し、接続を指示すると、外部端末装置22のCPU101は、ステップS83において、供給用データに基づいて、ローカルサーバ11にアクセスする。CPU101は、指示されたPCのアクセス先の接続キーが付加されたURLを、取得した供給用データの中から参照し、そのURLにアクセスする。

【0140】ステップS91において、外部端末装置22よりネットワーク21を介してアクセスされたローカルサーバ11のCPU51は、ステップS92において、ログイン画面データを、ネットワーク21を介して、外部端末装置22に供給する。

【0141】外部端末装置22のCPU101は、ステップS84において、ローカルサーバ11より供給されたログイン画面データを取得し、出力部112を制御して、ディスプレイ等に取得したログイン画面を表示させる。

【0142】図15は、ディスプレイに表示されたログイン画面の例を示す図である。



【0143】図15において、ディスプレイには、WEBブラウザ画面301が表示され、WEBブラウザ画面上にログイン画面302が表示される。ログイン画面302の中央には、外部端末装置22のユーザが有するローカルサーバ用識別情報に含まれるユーザ名を入力するユーザ名入力欄303、同様に、ローカルサーバ用識別情報に含まれるパスワードを入力するパスワード入力欄304、ユーザがマウス等により操作することで、入力されたユーザ名およびパスワードをローカルサーバ11に供給する処理の開始を指示するOKボタン305が設けられている。

【0144】ユーザは、キーボードまたはマウス等を操作して、ログイン画面302のユーザ名入力欄303に、ローカルサーバ11に登録してあるユーザ名を入力し、パスワード入力欄304に、ローカルサーバ11に登録してあるパスワードを入力し、OKボタン305を操作することで、ローカルサーバ11にローカルサーバ用識別情報を供給することができる。

【0145】図12に戻り、ユーザがログイン画面302に基づいて、ローカルサーバ用識別情報を入力して供給を指示すると、外部端末装置22のCPU101は、ステップS85において、通信部114を制御して、ネットワーク21を介して、入力されたローカルサーバ用識別情報をローカルサーバ11に供給する。

【0146】ローカルサーバ11のCPU51は、ステップS93において、通信部64を制御して、供給されたローカルサーバ用識別情報を取得し、ステップS94において、取得したローカルサーバ用識別情報について、記憶部63に記憶されているユーザに関する情報に基づいて、認証処理を行う。そして、認証処理が終了すると、CPU51は、ステップS95において、認証処理結果を外部端末装置22に供給する。外部端末装置22のCPU101は、供給された認証処理結果をステップS86において取得する。

【0147】なお、例えば、接続キーが変更された（ログイン画面のURLが変更された）後で、外部端末装置22が変更前の接続キーが付加されたURLにアクセスした場合、ローカルサーバ11は、エラー処理結果を外部端末装置22に供給し、接続を拒否する。外部端末装置22は、取得したエラー処理結果に基づいて、図16に示すように、「マイページから入りなおしてください」というエラーメッセージが表示されたエラー画面310を表示しているWEBブラウザ301をディスプレイに表示させる。

【0148】以上のように接続処理が行われることで、外部よりローカルサーバ11のログイン画面にアクセスするためには、認証サービスプロバイダ30の接続管理サーバ31に接続し、ログイン画面のURLを取得しなければならない。すなわち、ローカルサーバ11と通信を行うためには、認証サービスプロバイダ用識別情報およ

びローカルサーバ用識別情報が必要になり、より確実に不正なログインを抑制することができる。

【0149】また、ローカルサーバ11のユーザは、図8の設定画面251において、接続キーの設定を行うことにより、セキュリティのレベルを自由に調節させることができる。例えば、接続キーが無効に設定された場合、外部端末装置22は、ローカルサーバ11のログイン画面のURLを取得していれば、ローカルサーバ用識別情報のみでローカルサーバ11にログインすることができるし、固定の接続キーが有効に設定された場合、外部端末装置22は、1度ローカルサーバ11にログインするなどして、ローカルサーバ11のログイン画面の接続キーが付加されたURLを取得していれば、ローカルサーバ用識別情報のみでローカルサーバ11にログインすることができるし、決められた時間間隔で自動的に変更される接続キーに設定された場合、外部端末装置22は、接続キーが変更されるたびに認証サービスプロバイダ30の接続管理サーバ31にログイン画面のURLを要求しなければならない。

【0150】また、外部端末装置22のユーザが複数のローカルサーバにログインを許可されているような場合に置いても、ローカルサーバ11のログイン画面のURLを認証サービスプロバイダ30のアドレス管理サーバ32が管理し、要求に対応するローカルサーバに関する情報をリストで供給するので、外部端末装置22は、ログイン画面のURLを全て記憶しておく必要がなく、アドレス管理が容易である。

【0151】なお、以上においては、外部端末装置22がローカルサーバ11に接続する処理を説明したが、ネットワーク21に接続されている基地局24と無線通信を行い、ネットワーク21に接続されている携帯電話機23がローカルサーバ11に接続する場合も、その処理は同様に行われる。

【0152】次に、このとき接続管理サーバによって実行されるアクセス制御処理を、図17のフローチャートを参照して説明する。

【0153】最初に、ステップS131において、接続管理サーバ31のCPU151は、通信部164を制御して、外部端末装置22より認証サービスプロバイダ用識別情報を取得したか否かを判定することで、ローカルサーバ11への接続を要求されたか否かを判定し、要求されたと判定するまで待機する。

【0154】認証サービスプロバイダ用識別情報を取得し、ローカルサーバ11への接続を要求されたと判定した場合、CPU151は、ステップS132に進み、取得した認証サービスプロバイダ用識別情報について、認証処理を行う。CPU151は、認証処理として、取得した認証サービスプロバイダ用識別情報を認証サーバ33に供給し、識別情報の認証を要求する。そして、認証サーバ33より供給される認証結果を取得する。この処理

は、図12のステップS102およびステップS103に対応する。

【0155】CPU151は、ステップS133において、取得した認証結果に基づいて、認証サービスプロバイダ用識別情報が認証されたか否かを判定する。認証されたと判定した場合、CPU151は、ステップS134において、認証された識別情報をアドレス管理サーバ32に供給し、対応するローカルサーバ情報を要求する。この処理は、図12のステップS104に対応する。

【0156】そして、ステップS135において、CPU151は、アドレス管理サーバ32より要求したローカルサーバ情報を取得したか否かを判定し、取得したと判定するまで待機する。なお、所定の時間が経過した場合、または、エラーメッセージ等を取得した場合、CPU151は、アクセス制御処理を終了する。

【0157】要求したローカルサーバ情報を取得したと判定した場合、CPU151は、ステップS136に進み、取得したローカルサーバ情報に基づいて、供給用データを生成する。この処理は、図12のステップS106に対応する。

【0158】供給用データを生成したCPU151は、ステップS137に進み、生成した供給用データを、ネットワーク21を介して外部端末装置22に供給し、アクセス制御処理を終了する。この処理は、図12のステップS107に対応する。

【0159】また、ステップS133において、取得した認証結果に基づいて、認証サービスプロバイダ用識別情報が認証されていないと判定した場合、CPU151は、アクセス制御処理を終了する。

【0160】以上のようにして、ローカルサーバ11に接続した外部端末装置22は、ユーザの指示に基づいて、ネットワーク21を介してローカルサーバ11と通信を行い、ローカルサーバ11に備えられているアプリケーションプログラムに要求することで、ローカルサーバ11、またはLAN12に接続されている端末装置13等を制御することができる。

【0161】図18は、外部端末装置22およびローカルサーバ11が有するアプリケーションプログラムの様子を示す図である。図18を参照して、外部端末装置22とローカルサーバ11の通信の様子を説明する。

【0162】図18において、ローカルサーバ11には、WEBサーバ321が備えられており、このWEBサーバ321がHTTP等を利用した通信を行い、HTML文書や画像、音声等の各種の情報を、LAN12およびネットワーク21を介して外部端末装置22とやり取りする。

【0163】また、WEBサーバ321には、SSLを用いた暗号化を行うSSL322が連携されており、WEBサーバ321は、このSSL322を用いて、外部端末装置22に送信する送信データを暗号化したり、外部端末装置22より供給された暗号化されている受信データを復号した

りする。

【0164】また、ローカルサーバ11には、各種のアプリケーションプログラムを動作させるためのフレームワーク323が設けられており、WEBサーバを介して供給される外部端末装置22からの要求情報をアプリケーションプログラムに供給したり、アプリケーションプログラムの処理結果をWEBサーバ321を介して外部端末装置22に供給したりする。

【0165】図18においては、フレームワーク323には、図示せぬメールサーバに対してクライアント処理を行うメールクライアントプログラム331A、アドレスに関する情報を管理し、例えば、メールクライアントプログラム331Aと連携して動作するアドレス管理プログラム331B、ユーザの入力したスケジュールに関する情報を管理するスケジュール管理プログラム331C、および、その他のアプリケーションプログラムであるアプリケーションプログラム331D等が、搭載されている。フレームワーク323には、上述した以外にも、どのようなアプリケーションプログラムが搭載されていてもよく、また、搭載する数も、動作可能であれば、いくつでも良い。

【0166】フレームワーク323には、例えば、WEBコンテンツ324等が連携されており、フレームワーク323、またはフレームワーク323に搭載されたアプリケーションプログラムが必要とするヘルプ332Aや画像332Bなどを提供する。なお、WEBコンテンツ324は、上述した以外のコンテンツを備えていてもよい。

【0167】フレームワーク323には、JAVA（登録商標）関連モジュール325が連携されており、JAVA（登録商標）関連モジュール325は、フレームワーク323、およびフレームワーク323に搭載されているアプリケーションプログラムが必要とするJAVA（登録商標）言語に関する機能を提供する。

【0168】LAN12およびネットワーク21を介してローカルサーバ11と接続されている外部端末装置22は、WEBブラウザ341を有しており、WEBブラウザ341を用いて、HTTP等を利用した通信を行い、HTML文書や画像、音声等の各種の情報をローカルサーバ11とやり取りする。なお、図示は省略するが、WEBブラウザ341は、SSL機能を有しており、WEBサーバ321とSSLを用いた暗号通信をおこなうことができる。

【0169】以上のように、ローカルサーバ11と外部端末装置22は、WEBサーバ321とWEBブラウザ341により、HTTPを用いた通信を行う。

【0170】次に、ローカルサーバ11と外部端末装置22による通信処理を、図19のタイミングチャートを参照して説明する。ここでは、外部端末装置22がローカルサーバ11のアプリケーションプログラム331Dを制御する場合を説明する。

【0171】最初に、外部端末装置22のWEBブラウザ341は、ステップS151において、ユーザに指示された、画面表示や情報設定等の要求情報を、ネットワーク21およびLAN12を介して、ローカルサーバ11のWEBサーバ321に供給する。

【0172】WEBサーバ321は、ステップS161において、WEBブラウザ341より供給された要求情報を取得すると、ステップS162において、取得した要求情報をフレームワーク323に供給する。

【0173】フレームワーク323は、ステップS171において、その要求情報を取得すると、まず、ステップS172において、要求情報を供給した外部端末装置22のユーザの認証処理を実行する。認証処理は、例えば、要求情報を供給する際に用いられる接続キーや、要求情報に含まれるユーザの識別情報等により行われる。そして、ユーザが認証されると、フレームワーク323は、ステップS173において、取得した要求情報をXML (eXtensible Markup Language) ドキュメント化し、ステップS174において、XMLドキュメント化した要求情報を、対応するアプリケーションプログラム331Dに供給する。

【0174】図20は、フレームワーク323によりXMLドキュメント化された要求情報の例を示す図である。

【0175】図20において、上から1行目には、XMLのバージョンやエンコード方式等の基本情報が構成されている。3行目乃至6行目には、接続してきた装置の機種に関する情報、アドレスに関する情報等を含む接続情報が構成されている。

【0176】そして、上から7行目および9行目には、ユーザのIDおよびパスワード、並びに、そのユーザ用のファイルが存在するフォルダに関する情報等を含む、接続してきたユーザに関する情報が構成されている。また、8行目には、処理要求として入力された情報が構成されている。さらに、10行目乃至13行目には、アプリケーションがフレームワークに要求する事項を入力する場所が、XML文書の位置特定に用いる記法であるXPathにより記載されている。

【0177】以上のような、アプリケーションプログラムに供給される要求情報は、XMLドキュメント化されており、必要な情報は全て構成されるようにし、項目や行数などのデータ構造に関する制限は特にない。アプリケーションは、XMLドキュメントを取り扱うことができればよく、全てのアプリケーションプログラムが読み込み可能な共通化されたデータ構造を用意する必要はない。すなわち、例えば、フレームワーク323に新たにアプリケーションプログラムを追加する際も、その追加するアプリケーションプログラムが読み込むデータ構造が、先に搭載されているアプリケーションプログラムが読み込むデータ構造と共通である必要がなく、汎用性が高い。

【0178】従って、例えば、規格の変更などにより、最新のアプリケーションプログラムに必要なデータが、これまでのアプリケーションプログラムが利用していたデータ構造と異なる場合においても、フレームワークを変更することなく最新のアプリケーションプログラムを追加することができる。

【0179】図19に戻り、以上のようにXMLドキュメント化された要求情報を、アプリケーションプログラム331Dは、ステップS181において取得し、ステップS182において、取得した要求情報に基づいて、要求された固有の処理を行い、ステップS183において、要求情報に対応する応答情報を生成する。

【0180】アプリケーションプログラム331Dは、例えば、現在接続しているユーザ用のファイルのあるフォルダや要求内容などの使用する各種情報をフレームワーク323より供給されるXMLドキュメント化された要求情報から取得する。要求情報に関して、必要な情報解析はフレームワーク323が行っているため、アプリケーションプログラム331Dは、XMLドキュメント化された要求情報のXPathで記述された内容に従って、必要な情報を取得することができる。

【0181】そして、アプリケーションプログラム331Dは、ステップS184において、生成した応答情報に、画面表示に関する表示情報を付加した後、ステップS185において、その表示情報を付加した応答情報をフレームワーク323に供給する。

【0182】図21は、アプリケーションプログラム331Dよりフレームワーク323に供給される応答情報の例を示す図である。

【0183】図21において、上から1行目乃至9行目は、図20に示す内容と動揺であるので、その説明は省略する。10行目乃至14行目はフレームワーク323への要求が設定されており、16行目以降はアプリケーション固有の情報設定により構成されている。

【0184】アプリケーションプログラム331Dより出力される応答情報は、フレームワークを介して、要求情報の要求元である端末装置に供給される。従って、要求もとの端末装置の表示部の大きさ等により、表示される内容や形式が異なってしまう。しかしながら、アプリケーションプログラム331Dは、要求情報を供給した端末装置の機種が何かを特に必要でない限り意識せず、必要とされる情報を全てXMLドキュメントに追加するようにし、要求元である端末装置に最適な情報は、フレームワーク323が、アプリケーションプログラムより供給された応答情報を編集することにより、作成するようにする。

【0185】図19に戻り、以上のような、アプリケーションプログラム331Dに供給された応答情報は、ステップS175において、フレームワーク323に取得される。そして、フレームワーク323は、ステップS

176において、取得した応答情報に基づいて、要求情報の供給元に最適な出力用応答情報を生成し、ステップS177において、生成した出力用応答情報を供給する。すなわち、フレームワーク323は、応答情報を解析し、要求情報の供給元のWEBブラウザの種類等に応じて、最適な出力画像構成となるように、使用するXSL (eXtensible Stylesheet Language) を変更し、HTMLドキュメントを生成する。なお、フレームワーク323は、HTMLドキュメントを生成するとともに、応答情報を解析し、要求情報の供給元のWEBブラウザの種類等に応じて、出力画像が最適なレイアウトとなるように、使用するCSS (Cascading Style Sheet) を変更するようにしてもよい。

【0186】WEBサーバ163は、ステップS163において、フレームワーク323に供給された出力用応答情報を取得すると、ステップS164において、取得した出力用応答情報を要求情報の供給元である外部端末装置22に供給する。外部端末装置22は、ステップS152において、供給された出力用応答情報を取得し、ディスプレイ等に表示させる。

【0187】以上のようにして、ローカルサーバ11と外部端末装置22は、通信処理を行う。以上においては、外部端末装置22がローカルサーバ11のアプリケーションプログラム331Dを制御するように説明したが、これに限らず、外部端末装置22が制御するアプリケーションプログラムは、フレームワーク323に搭載されるアプリケーションプログラムであれば何でも良い。また、携帯電話機23がローカルサーバ11と通信処理を行う場合も、上述した場合と同様の処理が行われる。

【0188】次に、この通信処理において行われる、フレームワーク323によるアプリケーションプログラム管理処理を、図22のフローチャートを参照して説明する。

【0189】フレームワーク323は、ステップS201において、WEBサーバ321より要求情報を取得したか否かを判定し、取得したと判定するまで待機する。そして、取得したと判定した場合、フレームワーク323は、ステップS202に進み、取得した要求情報に対して、上述したような認証処理が必要か否かを判定する。

【0190】認証処理が必要と判定した場合、フレームワーク323は、ステップS203に進み、取得した要求情報に対して認証処理を行う。この処理は、図19のステップS172の処理に対応する。そして、フレームワーク323は、ステップS204に進み、要求情報の供給元のユーザが認証されたか否かを判定する。

【0191】認証されたと判定した場合、フレームワーク323は、ステップS205に進む。また、ステップS202において、認証処理が必要でないと判定した場合、フレームワーク323は、ステップS205に進

む。

【0192】ステップS205において、フレームワーク323は、取得した要求情報を、上述したように、XMLドキュメント化する。この処理は、図19のステップS173の処理に対応する。

【0193】要求情報をXMLドキュメント化したフレームワーク323は、ステップS206において、フレームワーク323に対応する要求情報が存在するか否かを判定し、存在すると判定した場合は、ステップS207に進み、要求情報に基づいて、必要な処理を行い、ステップS208に進む。ステップS206において、フレームワーク323に対応する要求情報が存在しないと判定した場合、フレームワーク323は、そのまま、ステップS208に進む。

【0194】ステップS208において、フレームワーク323は、アプリケーションプログラムに供給する要求情報が存在するか否かを判定し、存在すると判定した場合、ステップS209に進み、要求情報を対応するアプリケーションプログラムに供給する。この処理は、図19のステップS174の処理に対応する。

【0195】要求情報を供給したフレームワーク323は、ステップS210に進む。また、ステップS208において、アプリケーションプログラムに供給する要求情報が存在しないと判定した場合、フレームワーク323は、ステップS210に進む。ステップS210において、フレームワーク323は、要求情報を供給したアプリケーションプログラムより応答情報を取得したか否かを判定し、取得した、若しくは要求情報を供給していないと判定するまで待機する。

【0196】応答情報を取得した、または、要求情報を供給していないと判定した場合、フレームワーク323は、ステップS211に進む。また、ステップS204において、ユーザが認証されなかったと判定した場合、フレームワーク323は、ステップS211に進む。

【0197】ステップS211において、フレームワーク323は、取得した応答情報に基づいて、最適な出力用応答情報を生成する。この処理は、図19のステップS176の処理に対応する。最適な出力用応答情報を生成したフレームワーク323は、ステップS212に進み、生成した出力用応答情報をWEBサーバ321に供給し、アプリケーションプログラム管理処理を終了する。

【0198】以上のように通信処理を行い、外部端末装置22がローカルサーバ11のメールクライアントプログラム331Aを制御し、ローカルエリア10の外部からローカルサーバ11が受信した電子メールを参照する場合の処理を図23のタイミングチャートを参照して説明する。必要に応じて、図24乃至図26を適宜参照して説明する。

【0199】まず、図18に示すメールクライアントプログラム331Aは、ステップS251において、メー

ルサーバにアクセスし、まだ、受信していない電子メールである未受信メールを要求する。この処理は、予め登録された設定に基づいて、所定の時間間隔で、自動的に、繰り返し行われる。

【0200】メールサーバは、ステップS241において、メールクライアントプログラム331Aからの要求を取得すると、未受信メールがある場合、ステップS242において、要求された未受信メールをメールクライアントプログラム331Aに供給する。メールクライアントプログラム331Aは、ステップS252において、供給された電子メールを取得すると、ステップS253において、取得したメールを保存する。

【0201】ローカルエリア10の外部に存在する外部端末装置22は、ユーザの指示により、ステップS231において、ネットワーク21を介してローカルサーバ11にアクセスし、ユーザのアカウントに対応するメールを要求する。

【0202】図24は、外部端末装置22のディスプレイに表示されるメールクライアントトップ画面の例を示す図である。外部端末装置22がネットワーク21を介してローカルサーバ11にアクセスすると、上述したように認証処理が行われ、ローカルサーバ11のフレームワーク323は、メールクライアントプログラム331を動作させ、応答情報として、図24に示すようなGUI情報を外部端末装置22に供給する。外部端末装置22のCPU101は、出力部112を制御して、取得したGUI情報を、ディスプレイに表示されているWEBブラウザ画面301に表示させる。

【0203】図24において、WEBブラウザ画面301には、メールクライアントトップ画面351が表示されている。メールクライアントトップ画面351は、メールクライアントプログラム331Aが供給するGUIの中で最も上位のGUIであり、メールクライアントプログラム331Aが提供する各種の機能を実行させるボタンやリンクにより構成されている。すなわち、外部端末装置22のユーザは、メールクライアントトップ画面351を構成するリンクやボタンを操作することで、例えば、受信した電子メールの一覧を表示する受信箱を表示させたり、新規に電子メールを作成する画面を表示させたりすることができる。

【0204】メールクライアントトップ画面351の上部には、例えば、ユーザがマウス等により操作することで、新規の電子メールを作成する際に使用するアドレス帳の機能を動作させるアドレス帳ボタン352や、着信した電子メールの通知や転送先のアドレスを設定する機能を動作させる通知・転送設定ボタン353等を含む各種の機能を実行するボタン群が形成されている。

【0205】メールクライアントトップ画面351の左側には、メールクライアントプログラム331Aが提供する機能の一覧がリンクとして表示されている機能選択

欄354が構成されており、ユーザはマウス等によりこれらのリンクを指示することによっても各種の機能を実行させることができる。

【0206】また、メールクライアントトップ画面351の中央には、主な機能を動作させるボタン群およびその説明で構成されるメインメニュー欄355が形成されている。ユーザは、マウス等によりメインメニュー欄355に含まれるボタンを操作することによっても動作させる機能を選択することができる。

【0207】外部端末装置22のユーザは、以上のようなGUI画面に基づいて、メールクライアントプログラム331Aに対する要求を指示する。例えば、ユーザが受信箱の表示を要求すると、外部端末装置22は、その要求を、ステップS231において、メールクライアントプログラム331Aに供給する。この要求は、ローカルサーバ11に供給され、上述したように処理が行われ、メールクライアントプログラム331Aに供給される。

【0208】ステップS254において、その要求を取得したメールクライアントプログラム331Aは、上述したように、固有の処理を行い、保存済みメール一覧に関する情報を供給する。外部端末装置22は、ステップS232において、供給された保存済みメール一覧に関する情報を取得すると、図25に示すように、取得した保存済みメール一覧をディスプレイ等に表示させる。

【0209】図25は、外部端末装置22のディスプレイに表示された受信箱画面の例を示す図である。

【0210】外部端末装置22のディスプレイに表示されているWEBブラウザ画面301には、ローカルサーバ11のメールクライアントプログラム331Aより供給された保存済みメールの一覧を表示する受信箱画面361が構成されている。

【0211】受信箱画面361には、保存済みメールの一覧からなる受信メール選択欄362が構成されている。受信メール選択欄362は、未読または既読等の状態を示す項目、添付ファイルの有無を示す項目、電子メールの差出人の名前を示す項目、電子メールの件名を示す項目、および、着信日付または送信日付を示す項目等により構成されている。

【0212】受信メール選択欄362に表示されている内容のうち一部または全部がリンクにより構成されており、外部端末装置22のユーザは、例えば、受信メール選択欄362に表示されている電子メールの中から目的の電子メールの件名を、マウス等を操作することにより選択することにより、その電子メールの本文等を表示させることができる。

【0213】図23に戻り、ユーザが図25に示す受信メール選択欄362の中から目的のメールを選択すると、外部端末装置22は、ステップS233において、取得した保存済みメール一覧の中から、ユーザに指示された電子メールを選択し、その電子メールを供給するよう



に、メールクライアントプログラム331Aに要求する。

【0214】外部端末装置22のWEBブラウザ341からの要求は、WEBサーバ321およびフレームワーク323を介して、メールクライアントプログラム331Aに供給される。メールクライアントプログラム331Aは、ステップS256において、その要求を取得する。外部端末装置22からの要求を取得したメールクライアントプログラム331Aは、要求に対応する処理を行い、ステップS257において、要求された電子メールを外部端末装置22に供給する。

【0215】外部端末装置22は、ステップS234において、供給された電子メールを取得すると、ディスプレイ等に表示させる。

【0216】図26は、外部端末装置22のディスプレイに表示されたメール表示欄の例を示す図である。

【0217】図26において、WEBブラウザ画面301には、電子メールの本文等を表示するメール表示欄371が表示されている。メール表示欄371には、電子メールの本文の他に、電子メールの日付、差出人、宛先、同報、件名、および添付ファイルに関する情報等が表示される。

【0218】外部端末装置22のユーザは、このメール表示欄371を参照することにより、ローカルサーバ11において受信した電子メールの内容を見ることができる。これにより、例えば、ユーザは、自宅に設置されているローカルサーバ11のメールクライアント331Aが受信した電子メールを、外出先においても読むことが可能となる。

【0219】以上においては、メールクライアントプログラム331Aが受信した電子メールをローカルエリア10の外部において取得する処理を説明したが、これに限らず、外部端末装置22のユーザは、上述した処理と同様の処理を行うことにより、例えば、メールクライアントプログラム331Aに登録してあるアカウントで送信メールを作成したり、受信メールをフォルダに分類する等して整理したり、メールクライアントプログラム331Aに関する各種の設定を変更したりする等の、メールクライアントプログラム331Aが有する様々な機能を制御することができる。

【0220】また、以上においては、メールクライアントプログラム331Aが予め受信した電子メールを、外部端末装置22がユーザの指示に基づいてローカルサーバ11にアクセスし、取得するように説明したが、これに限らず、電子メールを受信した場合、自動的に、メールクライアントプログラム331Aが受信した旨を通知したり、受信したメールを外部端末装置22に転送したりするようにしてもよい。

【0221】その場合、ユーザは、メールクライアントプログラム331Aが電子メール受信時に、外部端末装

置22に対して、その旨を通知する、または受信した電子メールを転送するように予め設定しておく。外部端末装置22のユーザがマウス等により、外部端末装置22は、ディスプレイ等に、図24に示す通知・転送設定ボタン353を操作すると、図27に示すような、通知・転送に関する設定を行う通知・転送リスト表示欄を表示させる。

【0222】図27は、WEBブラウザ画面に表示されている通知・転送リスト表示欄を示す図である。

【0223】図27において、ディスプレイに表示されているWEBブラウザ画面301には、電子メール受信時の通知、または転送に関する設定の一覧が表示されている通知転送リスト表示欄381が表示されている。

【0224】通知・転送リスト表示欄381には、これまでに設定された通知および転送に関する設定情報の一覧の他に、ユーザがマウス等により操作することで、新規に設定情報を追加するGUIをWEBブラウザ画面301に表示させる追加ボタン382、ユーザがマウス等により操作することで、既に設定され、一覧に表示されている設定情報を削除するボタン等が設けられている。

【0225】外部端末装置22のユーザは、マウス等を用いて追加ボタン382を操作することにより、図28に示すような、通知または転送の設定を行うことができる通知・転送先設定欄をWEBブラウザ画面301に表示させ、新たな設定情報を作成することができる。

【0226】図28は、WEBブラウザ画面に表示されている通知・転送先設定欄を示す図である。

【0227】図28において、ディスプレイに表示されているWEBブラウザ画面301には、電子メール受信時の通知、または転送に関する設定を行うことができる通知転送先設定欄391が表示されている。

【0228】通知・転送先設定欄391には、ユーザがマウスまたはキーボード等を用いて通知・転送に関する設定情報の名前を入力するデータ名入力欄392、ユーザがマウス等を用いて、この設定情報が指示する処理の内容を選択するアクション選択欄393、ユーザがマウスまたはキーボード等を用いて、通知または転送先のアドレスを入力する通知・転送先アドレス入力欄394、および、ユーザがマウスまたはキーボード等を用いて、この設定情報に関するコメント等を入力するコメント入力欄395等が設けられている。また、これ以外にも、ユーザがマウス等を用いて操作することにより、入力した設定情報を新たに登録する追加ボタン等が構成されていても良い。

【0229】外部端末装置22のユーザは、この通知・転送先設定欄391に基づいて、通知または転送に関する設定情報を入力し、予め登録しておくことができる。

【0230】WEBブラウザ画面301に表示された、以上に示すようなGUI画面に基づいて、受信時に通知を行うようにする設定が予め行われている場合の処理を、図

29のタイミングチャートを参照して説明する。

【0231】図23に示す場合と同様に、ステップS291において、メールクライアントプログラム331Aが予め定められた時間間隔で、未受信メールを要求すると、メールサーバは、ステップS281において、その要求を取得し、ステップS282において、要求に対応する未受信メールが存在する場合、その未受信メールをメールクライアントプログラム331Aに供給する。

【0232】メールクライアントプログラム331Aは、ステップS292において、供給された電子メールを取得すると、ステップS293において、所得した新規受信メールを通知する通知メールを生成する。

【0233】そして、ステップS294において、メールクライアントプログラム331Aは、生成した通知メールを、ネットワーク21を介して、外部端末装置22に供給する。外部端末装置22は、ステップS271において、その通知メールを取得し、ディスプレイに表示されているWEBブラウザ301に、図26に示すようなメール表示欄371に取得した通知メールを表示する。

【0234】外部端末装置22が取得した通知メールには、メールクライアントプログラム331Aが電子メールを受信した旨を知らせるメッセージの他に、受信メールの件数、件名、または差出人などの、受信メールに関する主な情報、並びに、外部端末装置22が通知メールに対応する受信メールを取得する際にアクセスするアクセス先のURLが含まれていてもよい。

【0235】また、このURLはリンクになっていてもよく、ユーザがブラウザ画面301に表示されているこのURLを、マウス等を用いて選択することにより、外部端末装置22が、選択されたURLにアクセスし、対応する受信メールを表示するようにしてもよい。この場合、外部端末装置22が、ユーザにより選択されたURLにアクセスすると、ディスプレイに表示されているWEBブラウザ画面301には、対応する受信メールが表示された、図26に示すようなメール表示欄371が表示される。

【0236】このとき、通知メールに含まれるURLには、上述したような接続キーが含まれており、図1に示す認証サービスプロバイダ30による認証処理を省略することができる。また、同様に、通知メールに含まれるURLにローカルサーバ用識別情報が含まれるようにし、ローカルサーバ11による認証処理も省略するようにしてもよい。

【0237】以上のようにすることにより、外部端末装置22のユーザは、取得した通知メールに含まれるURLのリンクを、マウス等を用いて選択するだけで、ローカルサーバ11のメールクライアントプログラム331Aが受信したメールをディスプレイに表示させ、閲覧することができる。

【0238】なお、それとは逆に、URLに接続キーが含まれないようにして、外部端末装置22のユーザが受信

メールを閲覧する際に、認証サービスプロバイダ30の認証処理が必要であるようにしてもよい。

【0239】通知メールを取得し、ディスプレイ等に表示させた外部端末装置22は、ステップS272において、取得した通知メールに基づいてローカルサーバ11にアクセスし、ユーザの指示に対応するメールを、メールクライアントプログラム331Aに要求する。

【0240】メールクライアントプログラム331Aは、ステップS295において、その要求を取得すると、ステップS296において、要求されたメールを外部端末装置22に供給する。外部端末装置22は、ステップS273において、供給された電子メールを取得し、ディスプレイ等にその内容を表示する。

【0241】以上のように処理が行われることにより、外部端末装置22のユーザは、ローカルエリア10の外部より、メールクライアントプログラム331Aが受信したメールを閲覧することができる。

【0242】以上においては、外部端末装置22がネットワーク21を介してローカルサーバ11に接続し、メールクライアントプログラム331Aを制御するように説明したが、これに限らず、外部端末装置22が制御するアプリケーションプログラムは、メールクライアントプログラム331A以外にも、例えば、アドレス管理プログラム331Bやスケジュール管理プログラム331Cなどのように、ローカルサーバ11が有するアプリケーションプログラムであればなんでもよい。

【0243】図30は、WEBブラウザ画面301に表示されたアドレス帳トップ画面の例を示す図である。

【0244】図30において、ディスプレイに表示されたWEBブラウザ画面301には、アドレス管理サーバ331Bに対応するGUIのトップ画面であるアドレス帳トップ画面401が表示されている。

【0245】アドレス帳トップ画面401には、ユーザがマウス等を用いて操作することにより、アドレス管理プログラム331Bの主な機能の制御を行うGUIを表示させることができるメインメニュー画面402、および、ユーザがマウス等を用いて選択することにより、アドレス管理プログラム331Bが提供するアドレス帳機能に属する各種の機能の制御を行うGUIを表示させることができるリンク群である機能選択欄403が含まれている。

【0246】ユーザは、このアドレス帳トップ画面401の各種のボタンまたはリンクを操作することにより、アドレス帳を開いたり、アドレス情報を編集したりすることができる。

【0247】以上のようにして、外部端末装置22のユーザは、ローカルエリア10の外部より、ネットワーク21を介して、ローカルサーバ11に接続し、各種のアプリケーションプログラムを制御することができ、それにより、ローカルサーバ11、および、LAN12に接続

されている端末装置13等の動作を制御することができる。

【0248】なお、外部端末装置22が制御可能なローカルサーバ11のアプリケーションプログラムは、上述したもの以外にも、例えば、テレビジョン信号の録画や再生を行うアプリケーションプログラム、画像データの配信や編集などを行うアプリケーションプログラム、音楽データの録音や再生を行うアプリケーションプログラム等、図18に示すフレームワーク323に搭載されているアプリケーションプログラムであれば、どのような機能を有するアプリケーションプログラムであってもよい。

【0249】以上においては、外部端末装置22がローカルサーバ11に接続し、各種のアプリケーションプログラムを制御するように説明したが、携帯電話機23がローカルサーバ11に接続し、各種のアプリケーションプログラムを制御する場合も、上述した場合と同様の処理が行われる。

【0250】また、ローカルエリア10の外部の端末装置としては、上述したパーソナルコンピュータ等の外部端末装置22、および携帯電話機23の他に、例えば、通信機能を有するPDA(Personal Digital Assistance)などであってもよい。

【0251】以上において、図1に示すネットワークシステムを構成する、ローカルサーバ11、端末装置13、外部端末装置22、携帯電話機23、接続管理サーバ31、アドレス管理サーバ32、および認証サーバ33は、それぞれ1台ずつで構成されるように説明したが、これに限らず、複数台により構成されていてもよい。また、認証サービスプロバイダ30に設置された各サーバおよび各装置は、それぞれ、別体として構成してあるが、サービス全体、またはその一部が、一体化されていてもよい。

【0252】なお、以上において、システムとは、複数の装置により構成される装置全体を表すものである。

【0253】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0254】この記録媒体は、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク(フロッピディスクを含む)、光ディスク(CD-ROM(Compact Disk-Read Only Memory)、DVD(Digital Versatile Disk)を含む)、光磁気ディスク(MD(Mini-Disk)を含む)、もしくは半

導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMなどで構成される。

【0255】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0256】

【発明の効果】以上のように、本発明のネットワークシステムによれば、より安全に通信を行うことができる。

【0257】本発明の第1の情報処理装置および方法、記録媒体、並びにプログラムによれば、より安全に他の情報処理装置と通信を行うことができる。

【0258】本発明の第2の情報処理装置および方法、記録媒体、並びにプログラムによれば、他の情報処理装置間の通信を容易に管理することができる。

【図面の簡単な説明】

【図1】本発明を適用したネットワークシステムの構成例を示す図である。

【図2】図1に示すローカルサーバの構成例を示すブロック図である。

【図3】図1に示す外部端末装置の構成例を示すブロック図である。

【図4】図1に示す接続管理サーバの構成例を示すブロック図である。

【図5】図1に示すアドレス管理サーバの構成例を示す図である。

【図6】図1に示すローカルサーバによるローカルサーバ情報登録処理を説明するフローチャートである。

【図7】図1に示すアドレス管理サーバによるローカルサーバ情報登録処理を説明するフローチャートである。

【図8】接続キーに関する設定を行う設定画面の様子の例を示す図である。

【図9】接続キーに関する設定を行う設定画面の様子の他の例を示す図である。

【図10】図1に示すローカルサーバによるローカルサーバ情報更新処理を説明するフローチャートである。

【図11】図1に示すアドレス管理サーバによるローカルサーバ情報更新処理を説明するフローチャートである。

【図12】外部端末装置からローカルサーバにログインする処理を説明するタイミングチャートである。

【図13】ログイン画面の例を示す図である。

【図14】ローカルサーバ一覧画面の例を示す図である。

【図15】ログイン画面の例を示す図である。

【図16】エラー画面の例を示す図である。

【図17】接続管理サーバによるアクセス制御処理を説

明するフローチャートである。

【図18】アプリケーションプログラムの様子を示す図である。

【図19】ローカルサーバと外部端末装置による通信処理を説明するタイミングチャートである。

【図20】フレームワークによりXMLドキュメント化された要求情報の例を示す図である。

【図21】フレームワークに供給される応答情報の例を示す図である。

【図22】フレームワークによるアプリケーションプログラム管理処理を説明するフローチャートである。

【図23】ローカルエリアの外部からローカルサーバが受信した電子メールを参照する場合の処理を説明するタイミングチャートである。

【図24】メールクライアントトップ画面の例を示す図である。

【図25】受信箱画面の例を示す図である。

【図26】メール表示欄の例を示す図である。

【図27】通知・転送リスト表示欄を示す図である。

【図28】通知・転送先設定欄を示す図である。

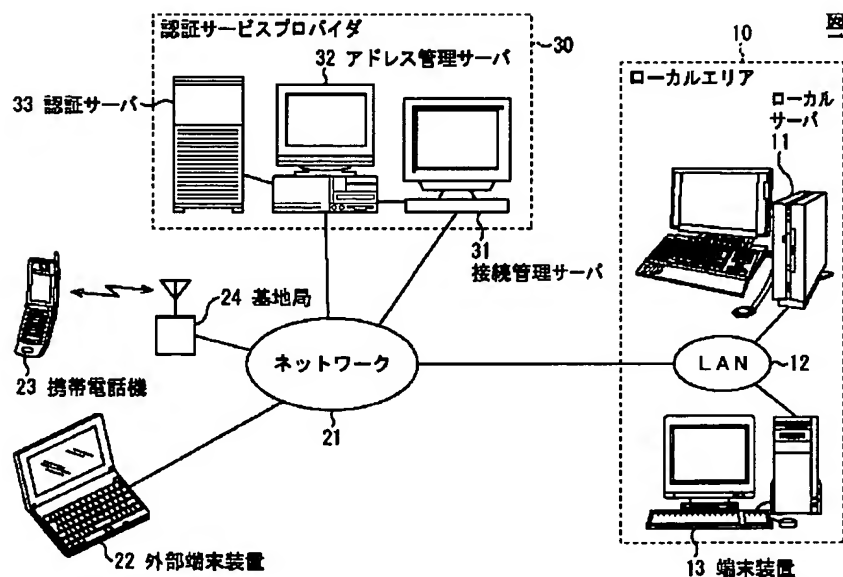
【図29】受信時に通知を行うようにする設定が予め行われている場合の処理を説明するタイミングチャートである。

【図30】アドレス帳トップ画面の例を示す図である。

【符号の説明】

11 ローカルサーバ、12 LAN、13 端末装置、21 ネットワーク、22 外部端末装置、23 携帯電話機、24 基地局、30 認証サービスプロバイダ、31 接続管理サーバ、32 アドレス管理サーバ、33 認証サーバ、321 WEBサーバ、322 SSL、323 フレームワーク、324 WEBコンテンツ、325 JAVA（登録商標）関連モジュール、331A メールクライアントプログラム、331B アドレス管理プログラム、331C スケジュール管理プログラム、331D アプリケーションプログラム

【図1】



【図2】

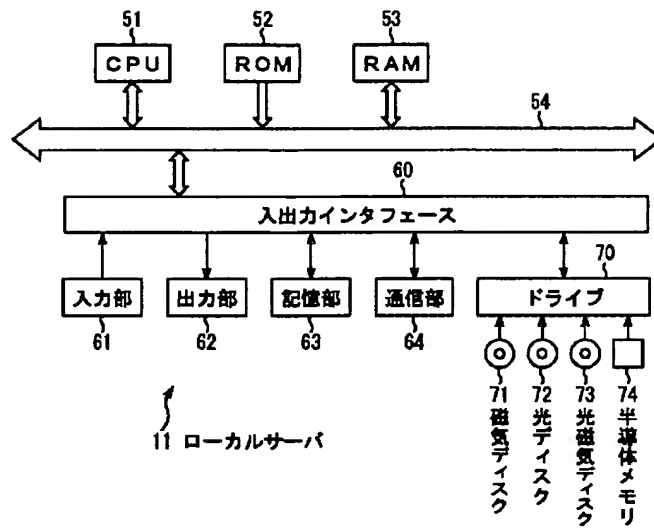


図2

【図3】

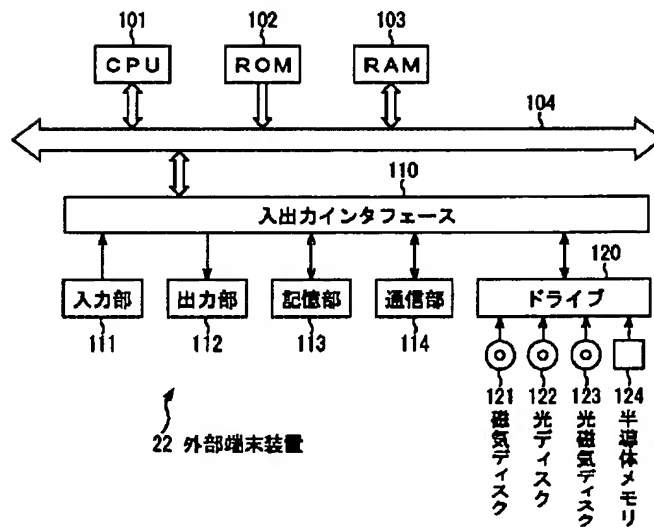


図3



【図4】

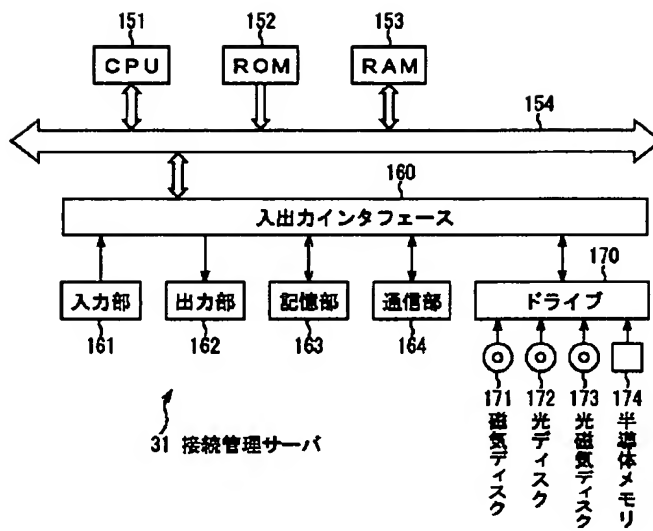


図4

【図5】

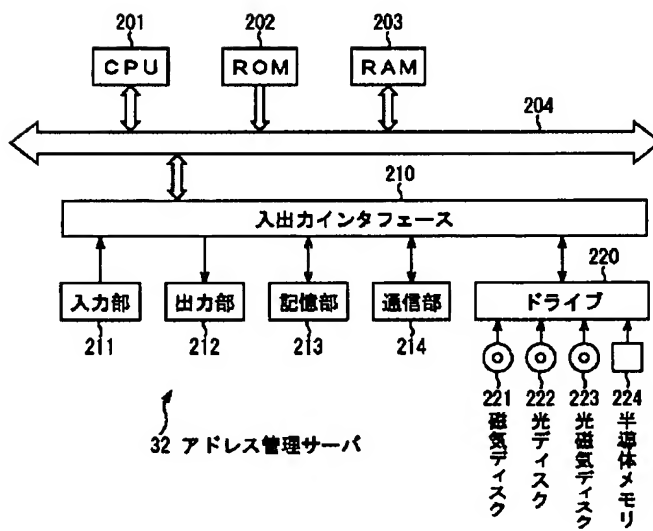
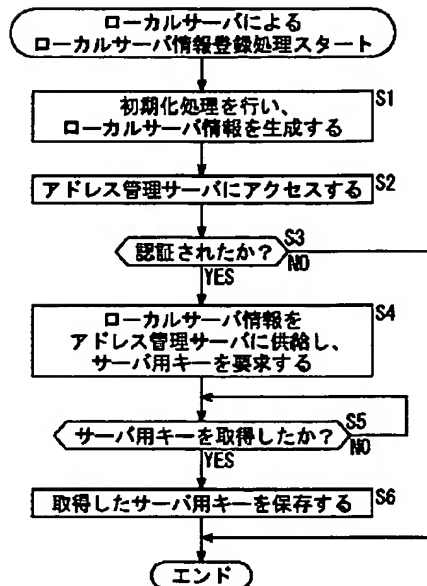


図5

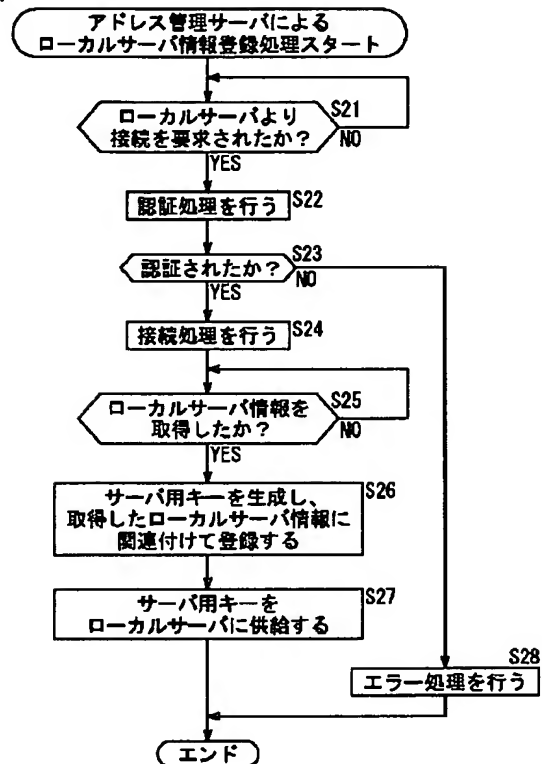
【図6】

図6

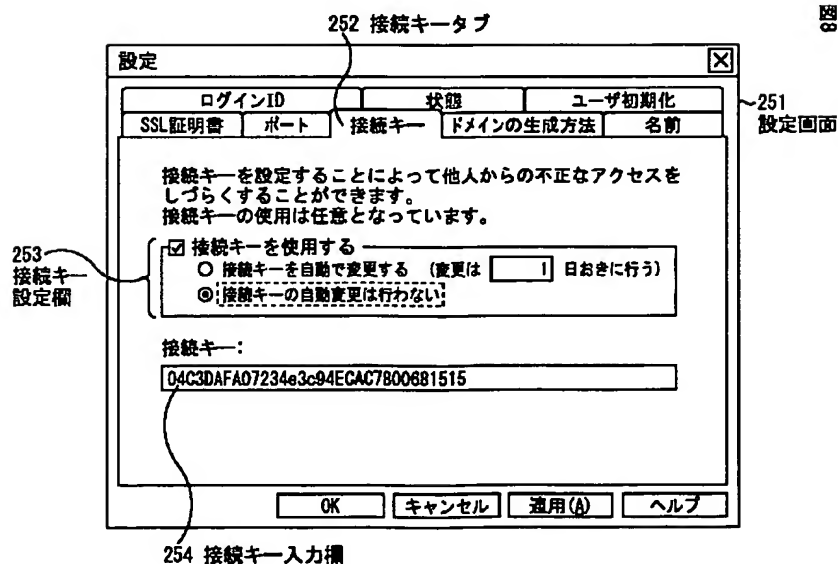


【図7】

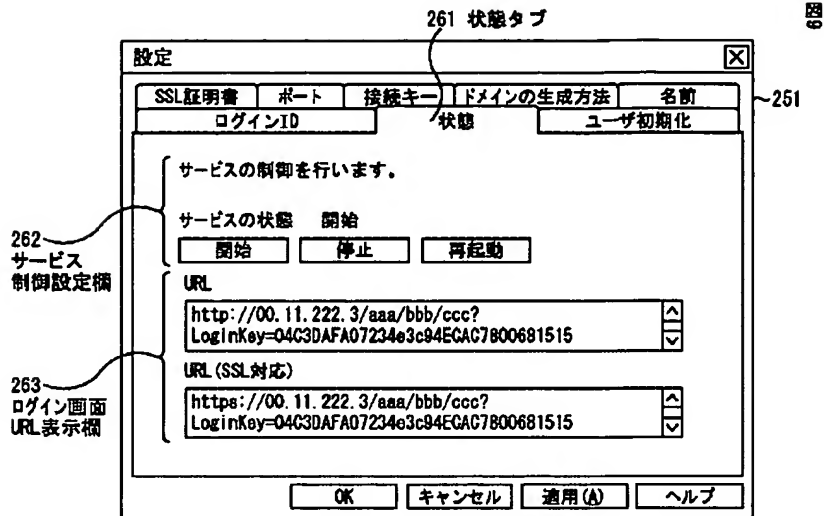
図7



【図8】

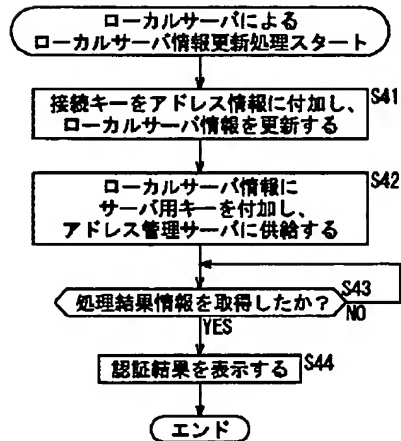


【図9】



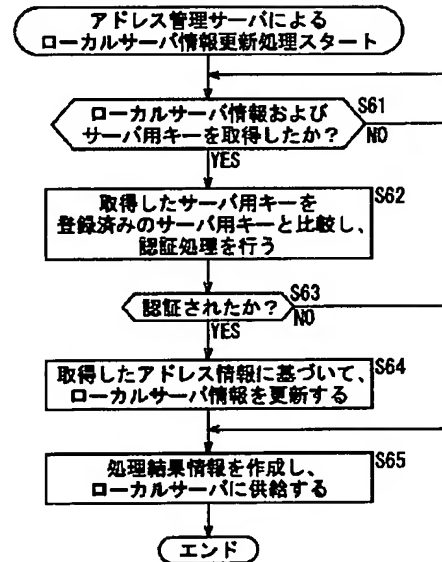
【図10】

図10

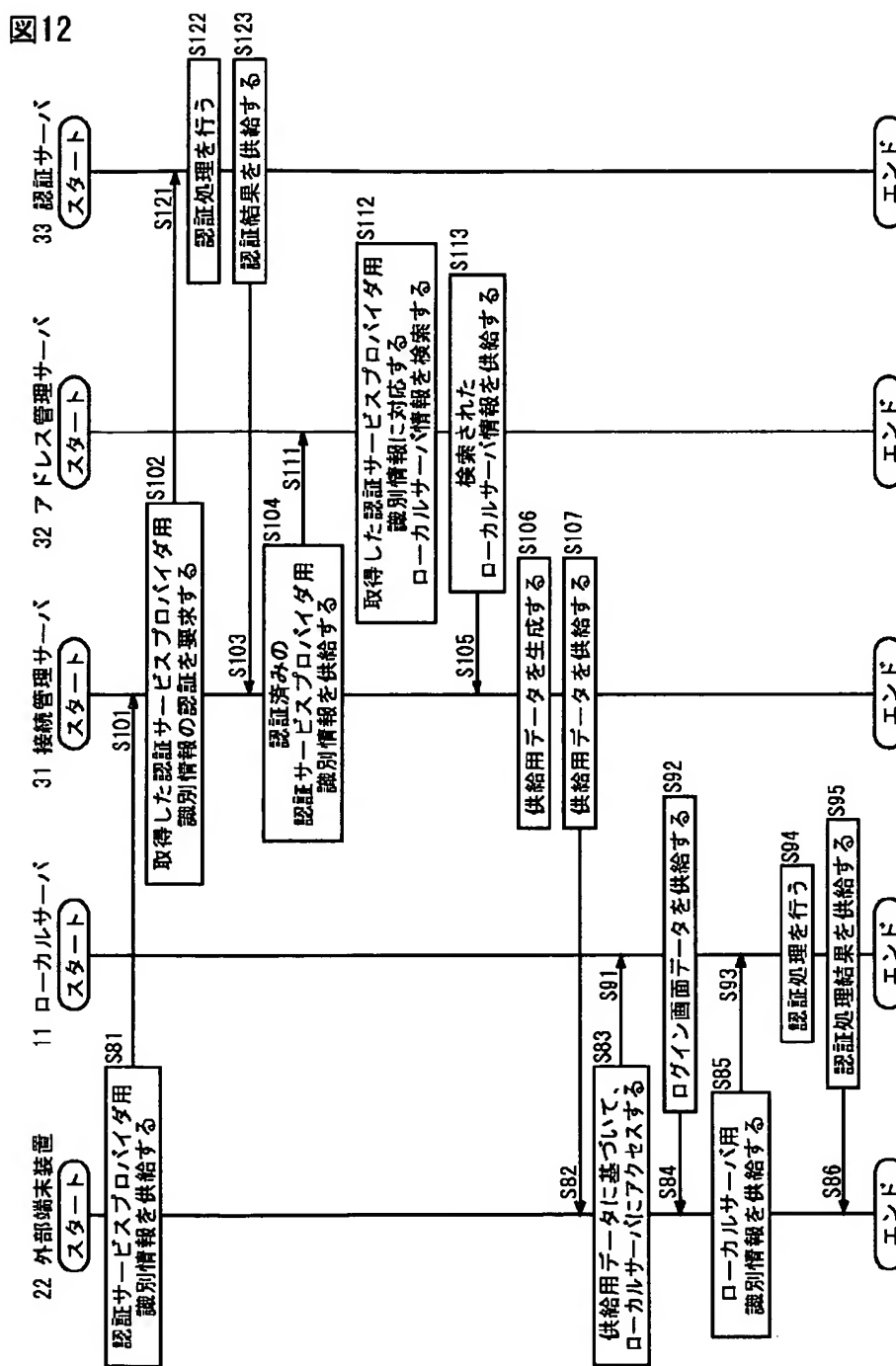


【図11】

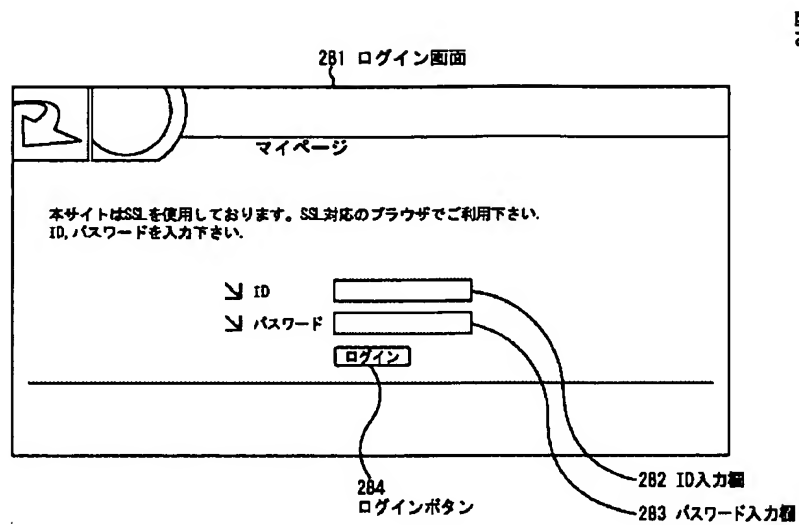
図11



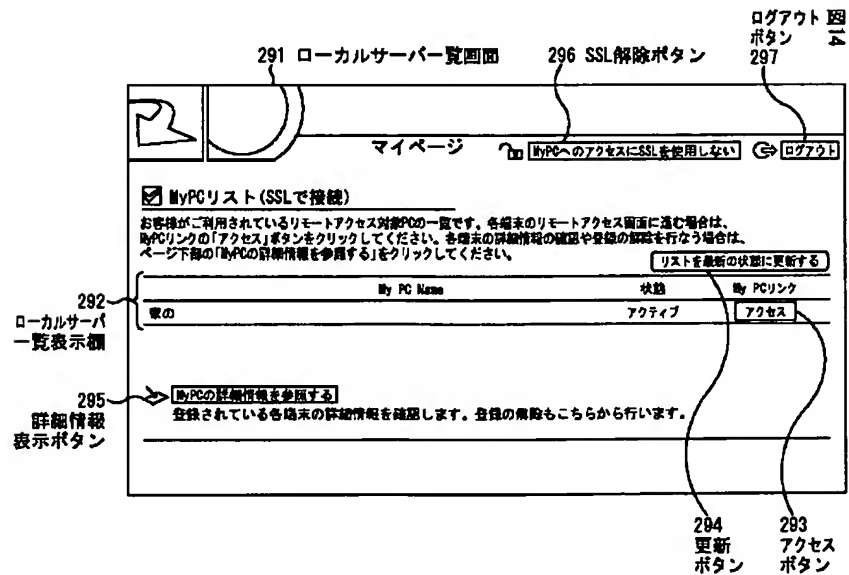
【図12】



【図13】

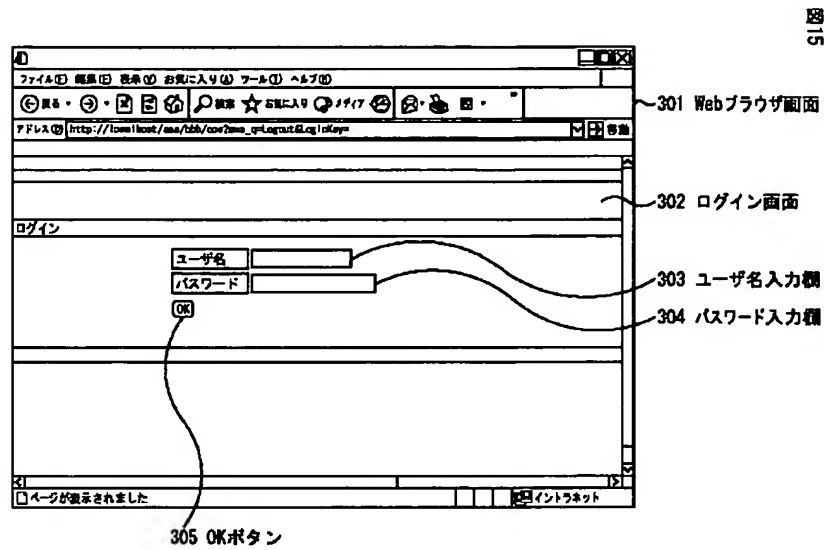


【図14】

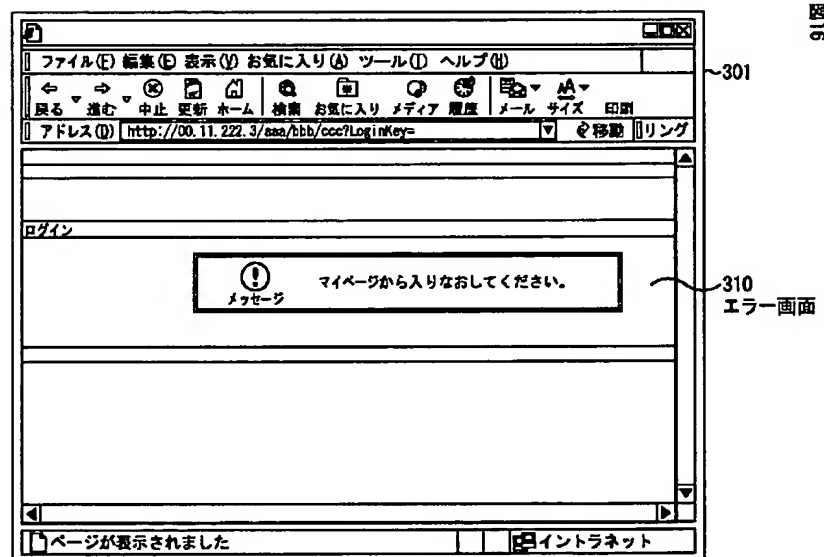




【図15】

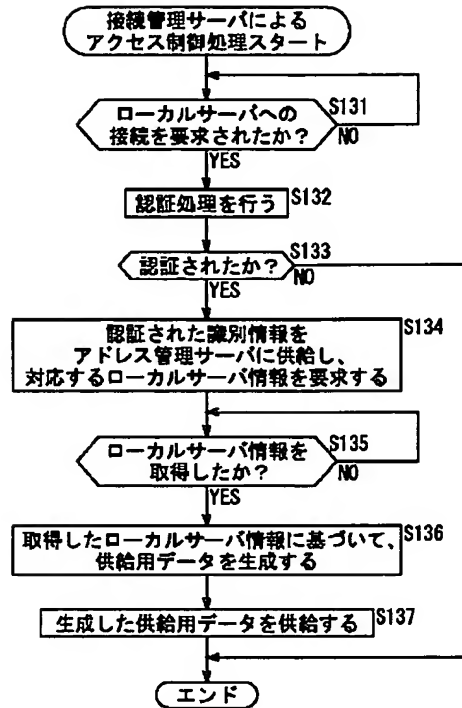


【図16】

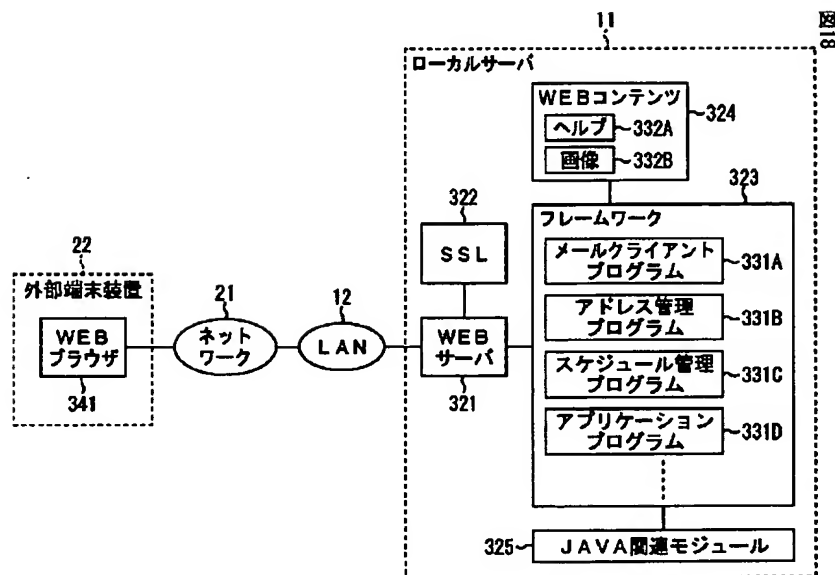


【図17】

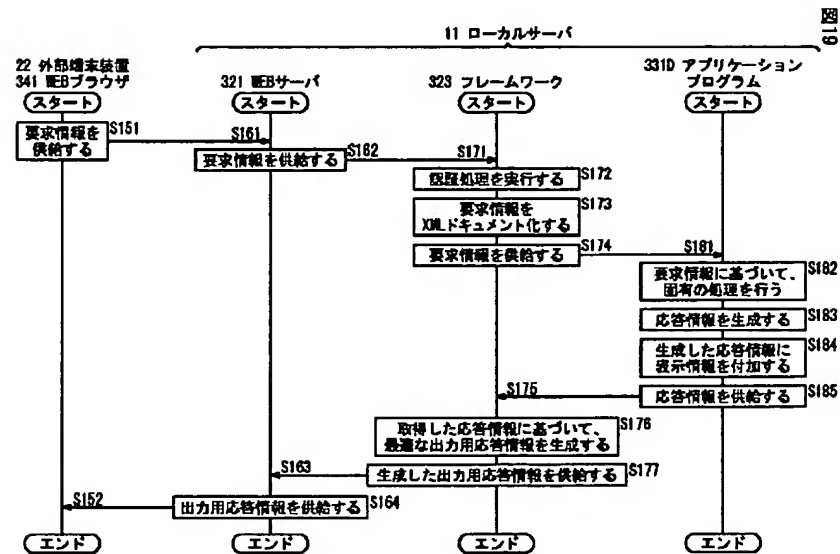
図17



【図18】



【図19】



【図20】

図20

```

<?xml version="1.0" encoding="UTF-8"?>
<app>
  <header cache-control="max-stale=0" host="11.22.33.44:500" user-agent="XXXXXX/1.0/5000i/c10" />
  <device media="html" maker="XXXXXX" version="1.0" name="S0001" cache="10" un_sslink="true" />
  <request uri="/xxx/yyy/zzz:jsessionid=yapu3corh1" sessionid="jsessionid=yapu3corh1" method="GET"
  remote_addr="xxx.x.x.x" remote_host="xxx.x.x.x" class="xx/xx/xxxx" />
  <dir user="D:/SSSS/xxx/zzz/demo" conf="D:/SSSS/xxx/zzz/conf" web="D:/SSSS/xxx/zzz/web/html" />
  <input q="View" id="1011067307834" />
  <user ID="demo" Password="demo" LoginKey="testkey" />
  <help url="help.html" />
  <message display="false" />
  <output xsl="output.xsl" />
  <redirect send="false" uri="/xxx/yyy/zzz:jsessionid=yapu3corh1" />
</app>

```

【図21】

図21

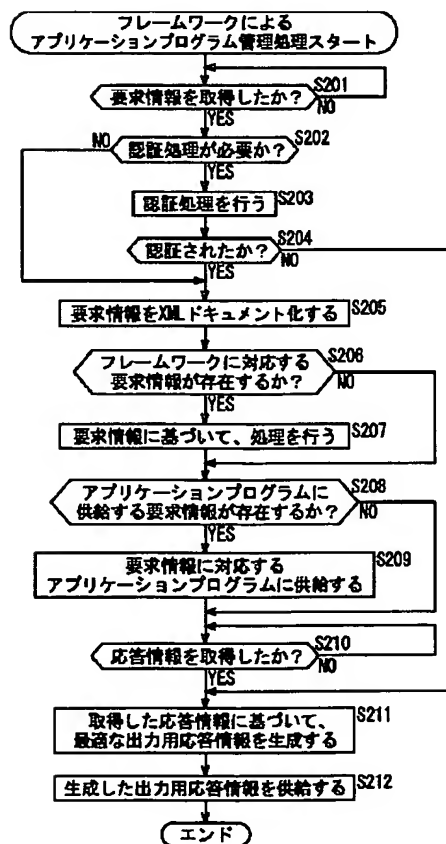
```

<?xml version="1.0" encoding="UTF-8"?>
<app>
  <header cache-control="max-stale=0" host="11.22.33.44:500" user-agent="XXXXXX/1.0/S0001/c10" />
  <device media="html" maker="XXXXXX" version="1.0" name="S0001" cache="10" un_sallink="true" />
  <request uri="/xxx/yyy/zzz:jsessionid=yapu3corh1" sessionid=":jsessionid=yapu3corh1" method="GET"
  remote_addr="xxx.x.x.x" remote_host="xxx.x.x.x" class="xx/xx/xxxx" />
  <dir user="D:/SSSS/xxx/zzz/demo" conf="D:/SSSS/xxx/zzz/conf" web="D:/SSSS/xxx/zzz/web/ctml" />
  <input q="View" id="1011067307834" />
  <user ID="demo" Password="demo" LoginKey="testkey" />
  <help url="help_aaa.html" />
  <message display="true">
    <line id="MSG-1" />
  </message>
  <output xsl="output_aaa.xsl" />
  <redirect send="false" uri="/xxx/yyy/zzz:jsessionid=yapu3corh1" />
  <menu>
    <folderlist>
      .
      .
      .
    </menu>
  </app>

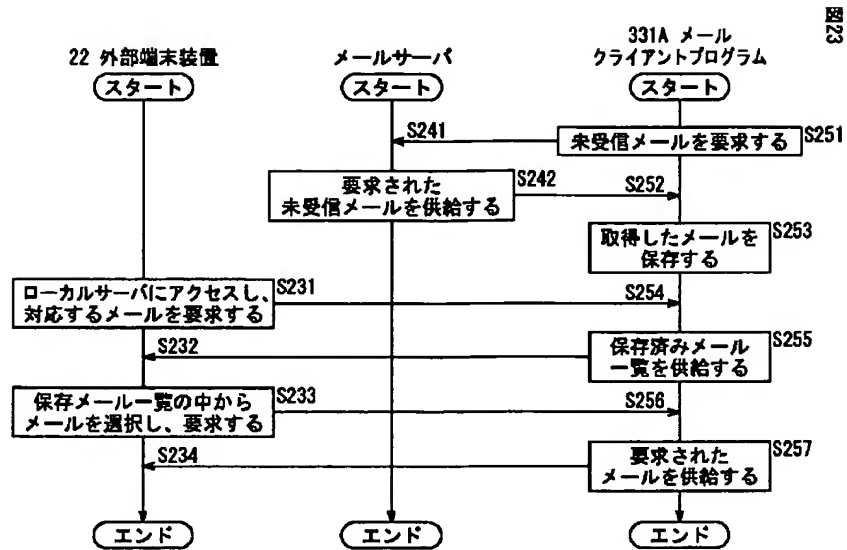
```

【図22】

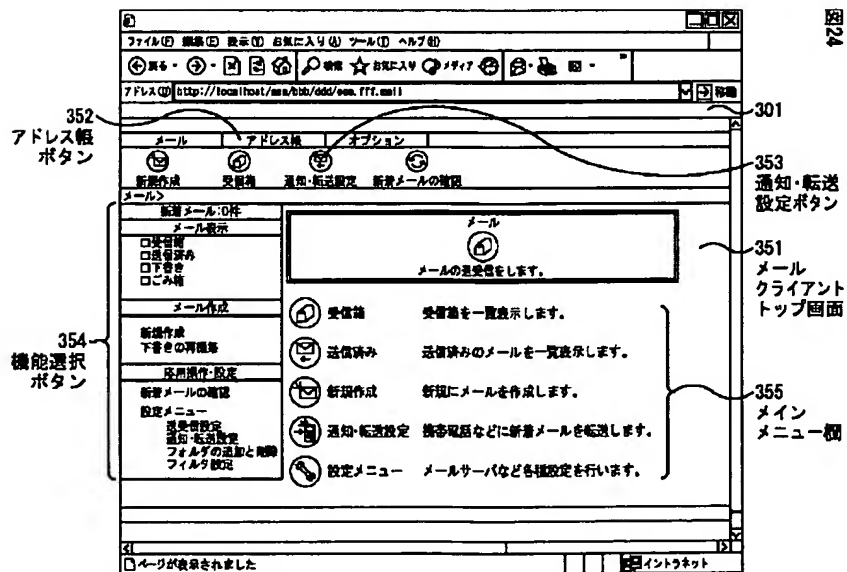
図22



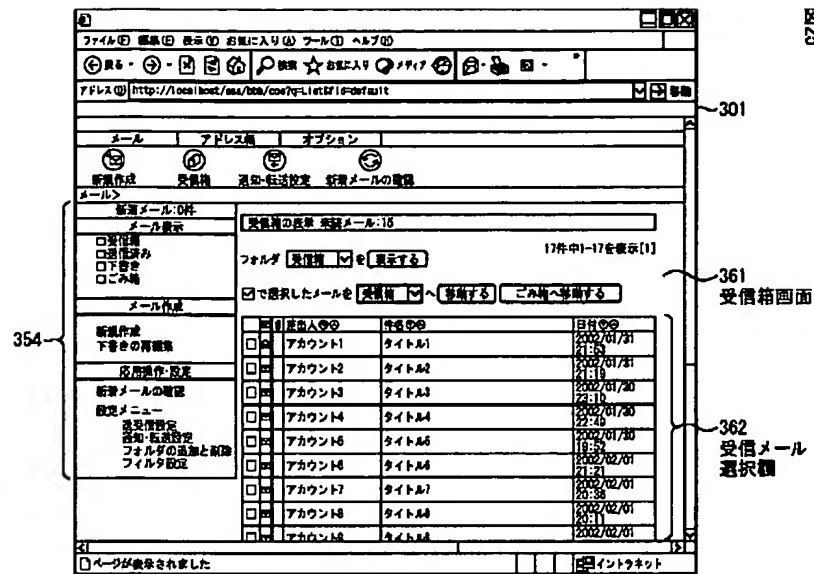
【図23】



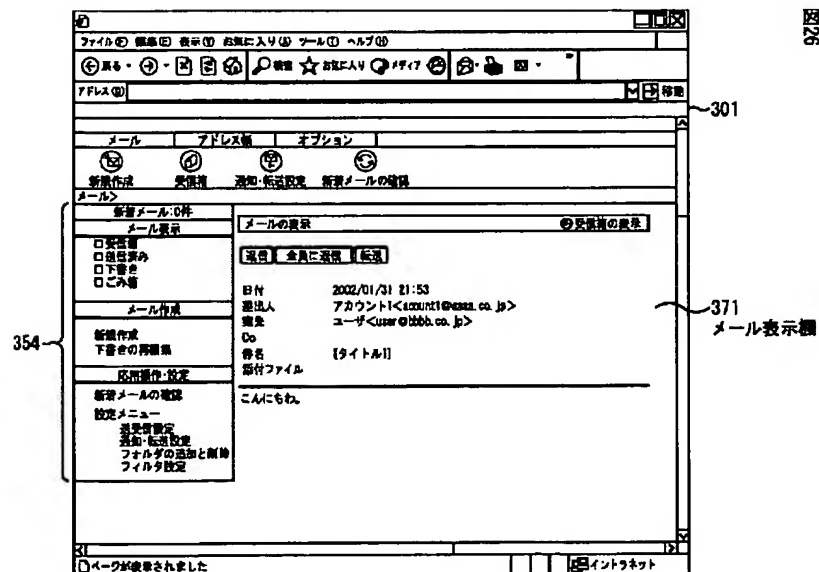
【図24】



【図25】

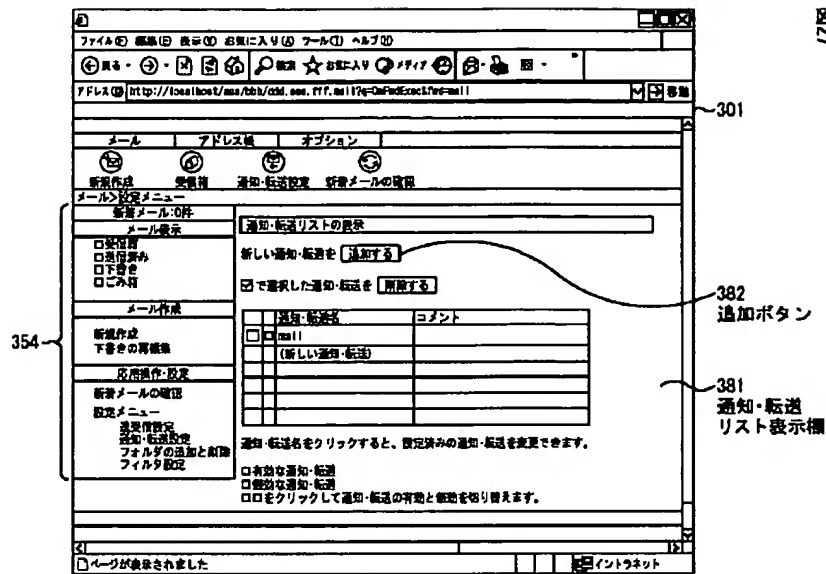


【図26】

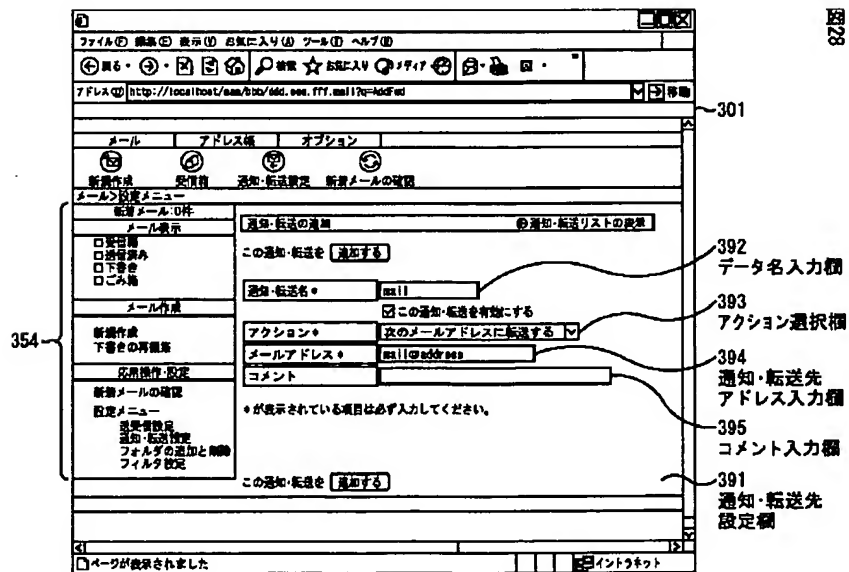




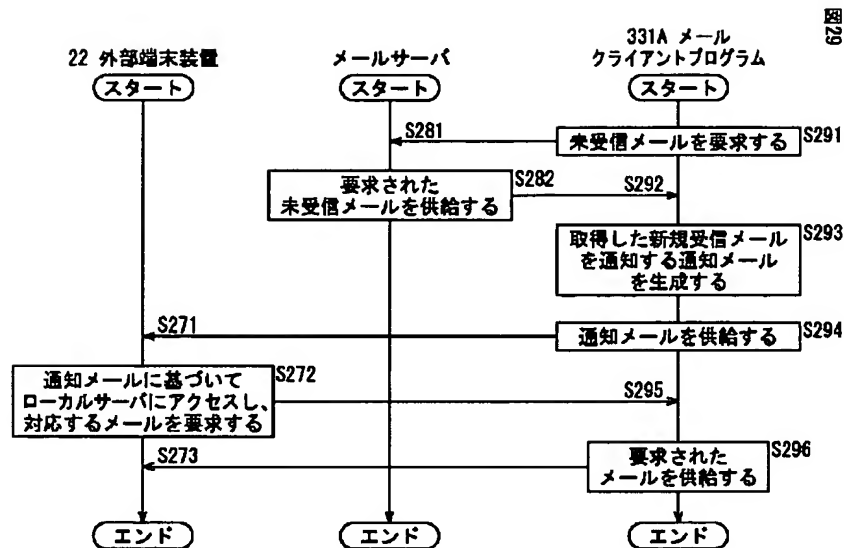
【図27】



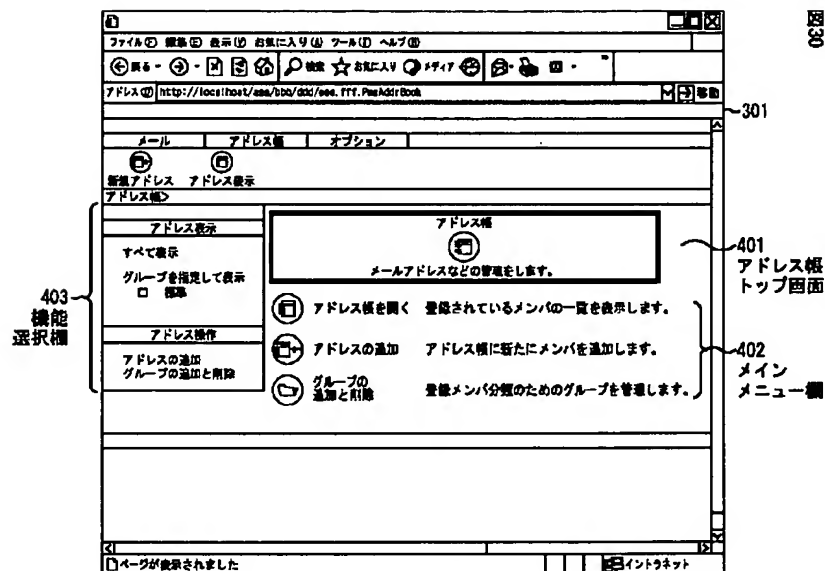
【図28】



【図29】



【図30】



フロントページの続き

(72)発明者 東原 正和  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 西浦 健一郎  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 遠藤 悦伸  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

Fターム(参考) 5B085 AE04 BC00